FIG. 1

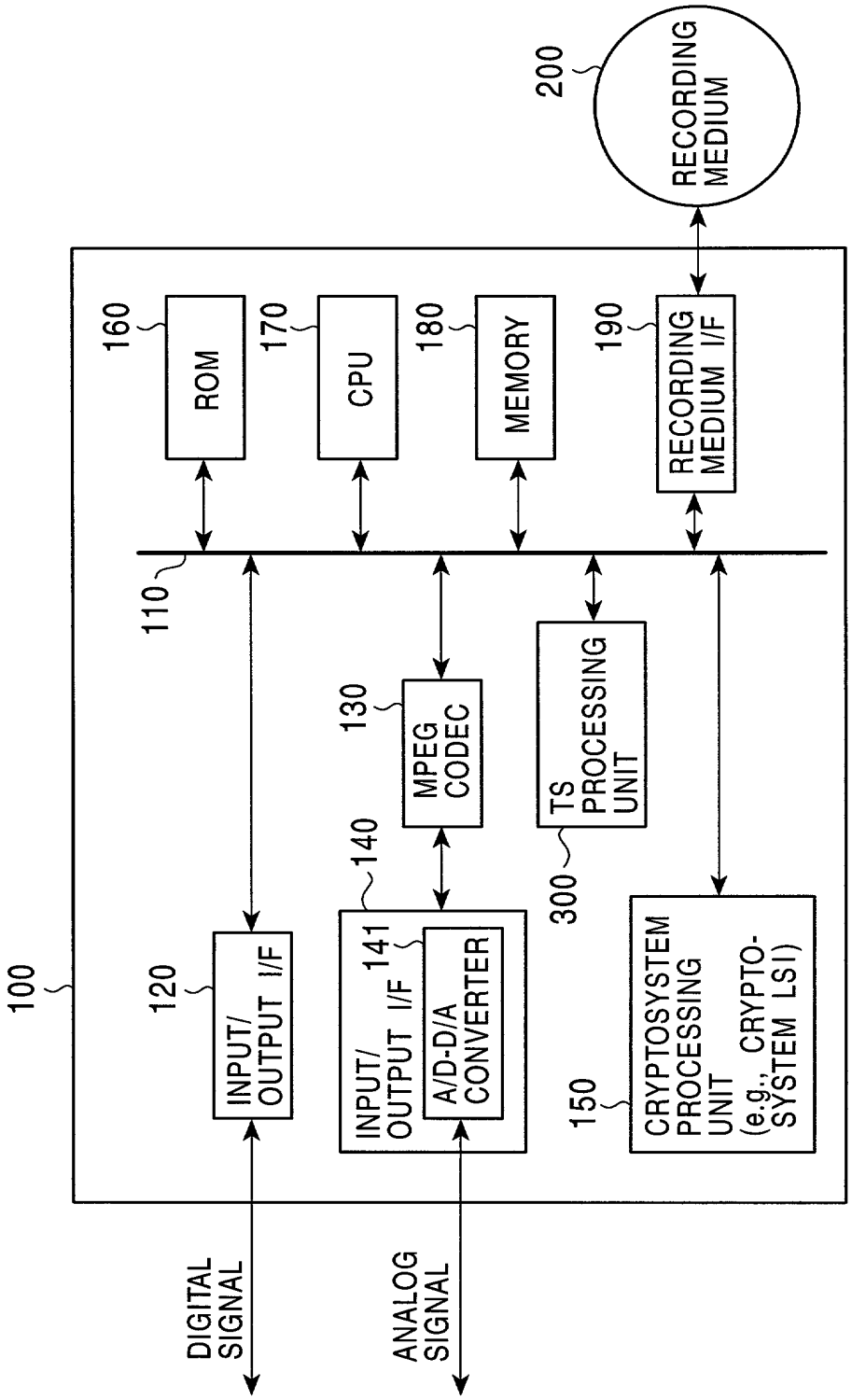

200
RECORDING MEDIUM
160
ROM
170
CPU
180
MEMORY
190
RECORDING MEDIUM I/F
110
130
MPEG CODEC
TS PROCESSING UNIT
300
140
141
INPUT/ OUTPUT I/F
A/D-D/A CONVERTER
120
INPUT/ OUTPUT I/F
150
CRYPTOSYSTEM PROCESSING UNIT (e.g., CRYPTO-SYSTEM LSI)
100
DIGITAL SIGNAL
ANALOG SIGNAL

FIG. 2

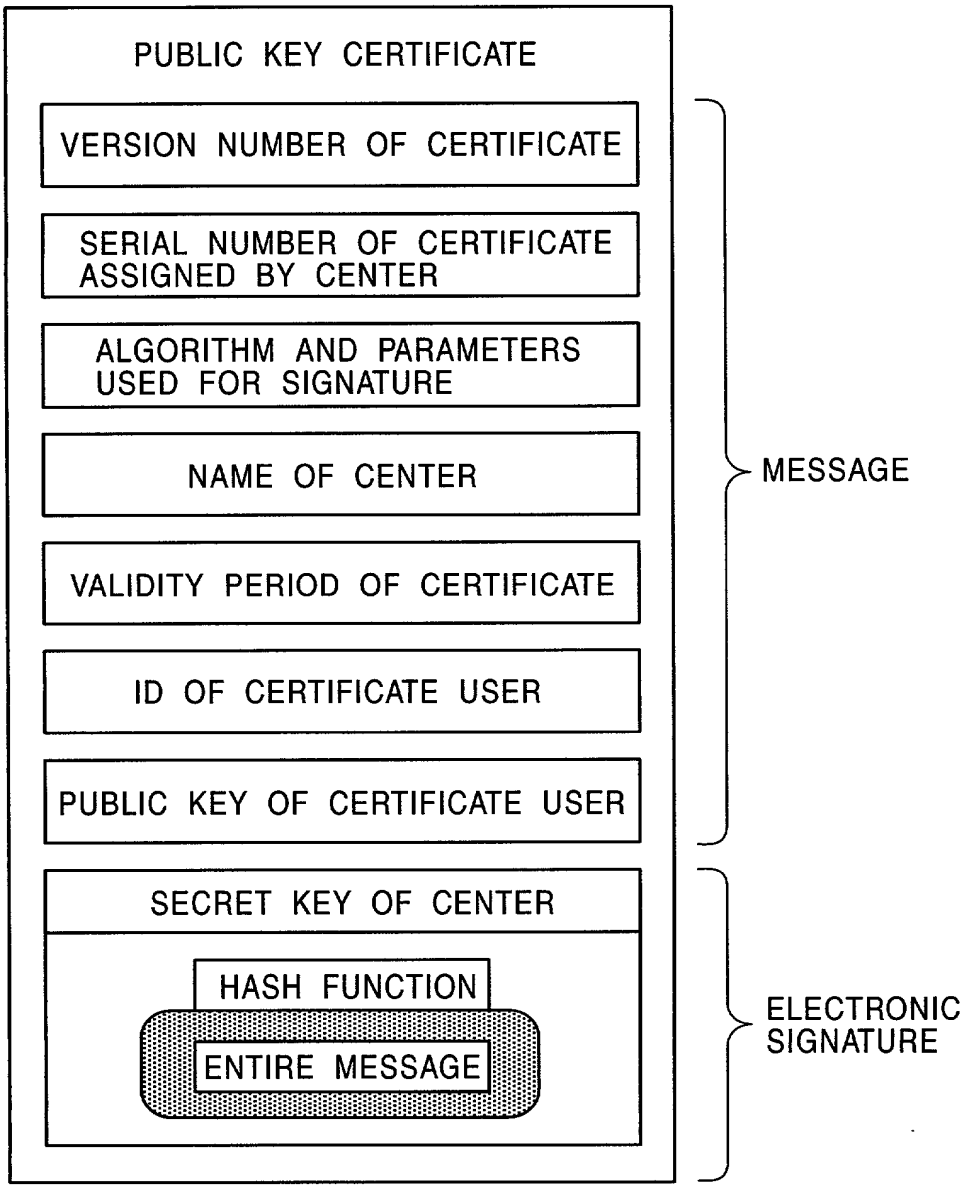

PUBLIC KEY CERTIFICATE
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ASSIGNED BY CENTER
ALGORITHM AND PARAMETERS USED FOR SIGNATURE
NAME OF CENTER
VALIDITY PERIOD OF CERTIFICATE
ID OF CERTIFICATE USER
PUBLIC KEY OF CERTIFICATE USER
MESSAGE
SECRET KEY OF CENTER
HASH FUNCTION
ENTIRE MESSAGE
ELECTRONIC SIGNATURE

FIG. 3A

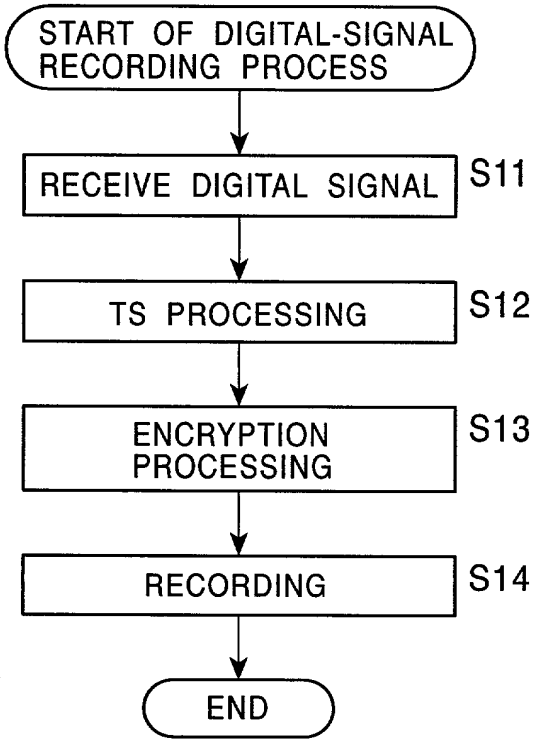

START OF DIGITAL-SIGNAL RECORDING PROCESS
RECEIVE DIGITAL SIGNAL
S11
TS PROCESSING
S12
ENCRYPTION PROCESSING
S13
RECORDING
S14
END

FIG. 3B

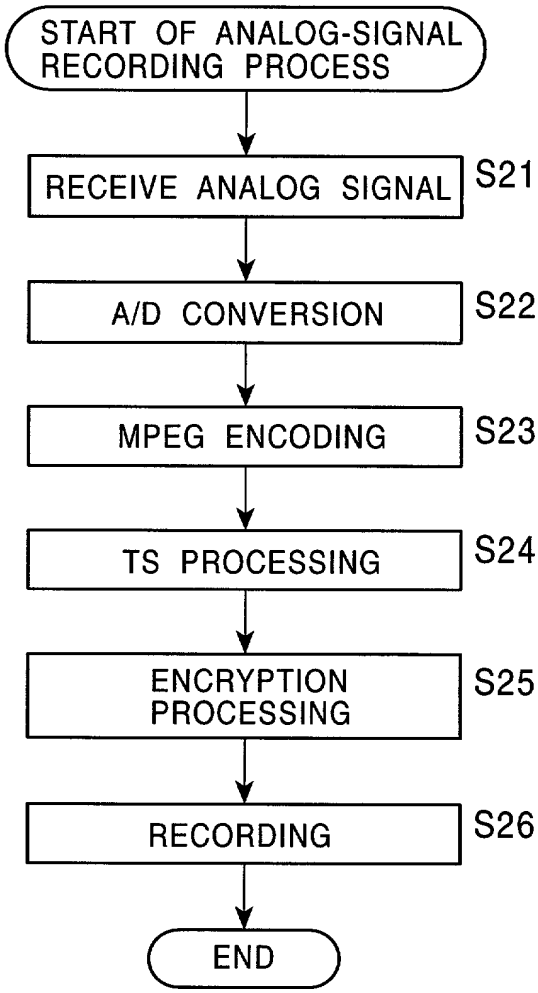

START OF ANALOG-SIGNAL RECORDING PROCESS
RECEIVE ANALOG SIGNAL
S21
A/D CONVERSION
S22
MPEG ENCODING
S23
TS PROCESSING
S24
ENCRYPTION PROCESSING
S25
RECORDING
S26
END

FIG. 4A

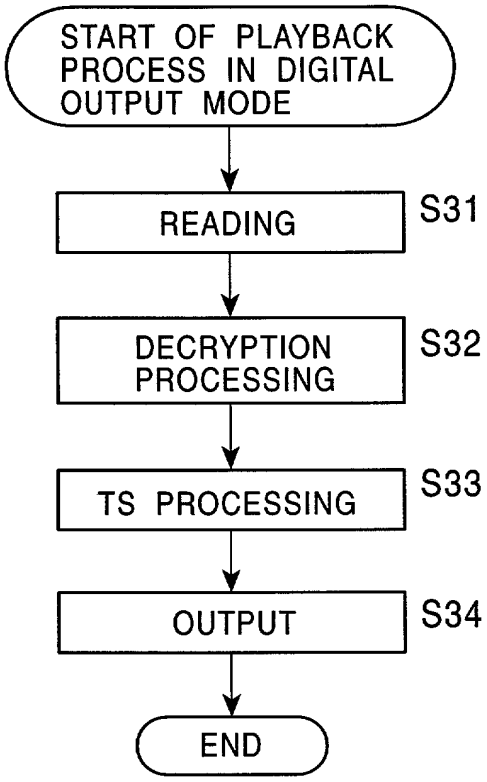

START OF PLAYBACK PROCESS IN DIGITAL OUTPUT MODE
READING
S31
DECRYPTION PROCESSING
S32
TS PROCESSING
S33
OUTPUT
S34
END

FIG. 4B

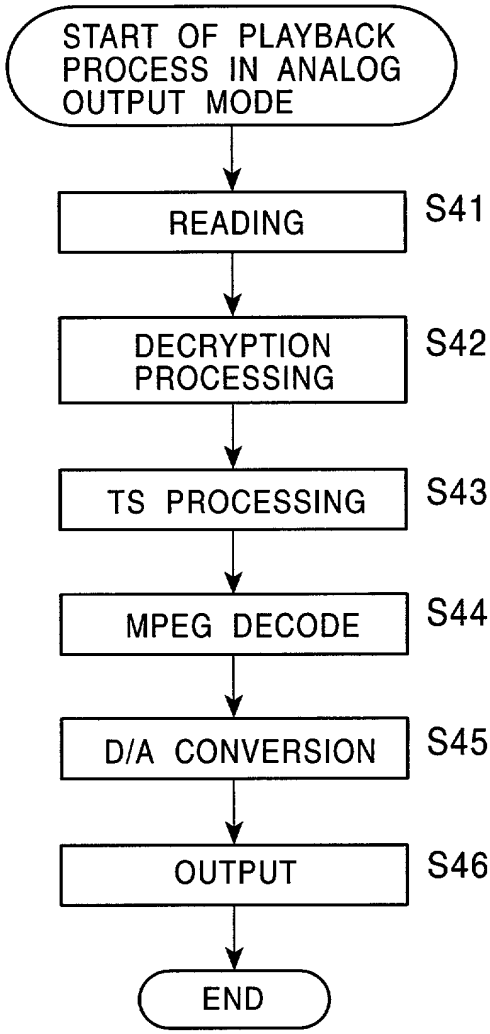

START OF PLAYBACK PROCESS IN ANALOG OUTPUT MODE
READING
S41
DECRYPTION PROCESSING
S42
TS PROCESSING
S43
MPEG DECODE
S44
D/A CONVERSION
S45
OUTPUT
S46
END

FIG. 5

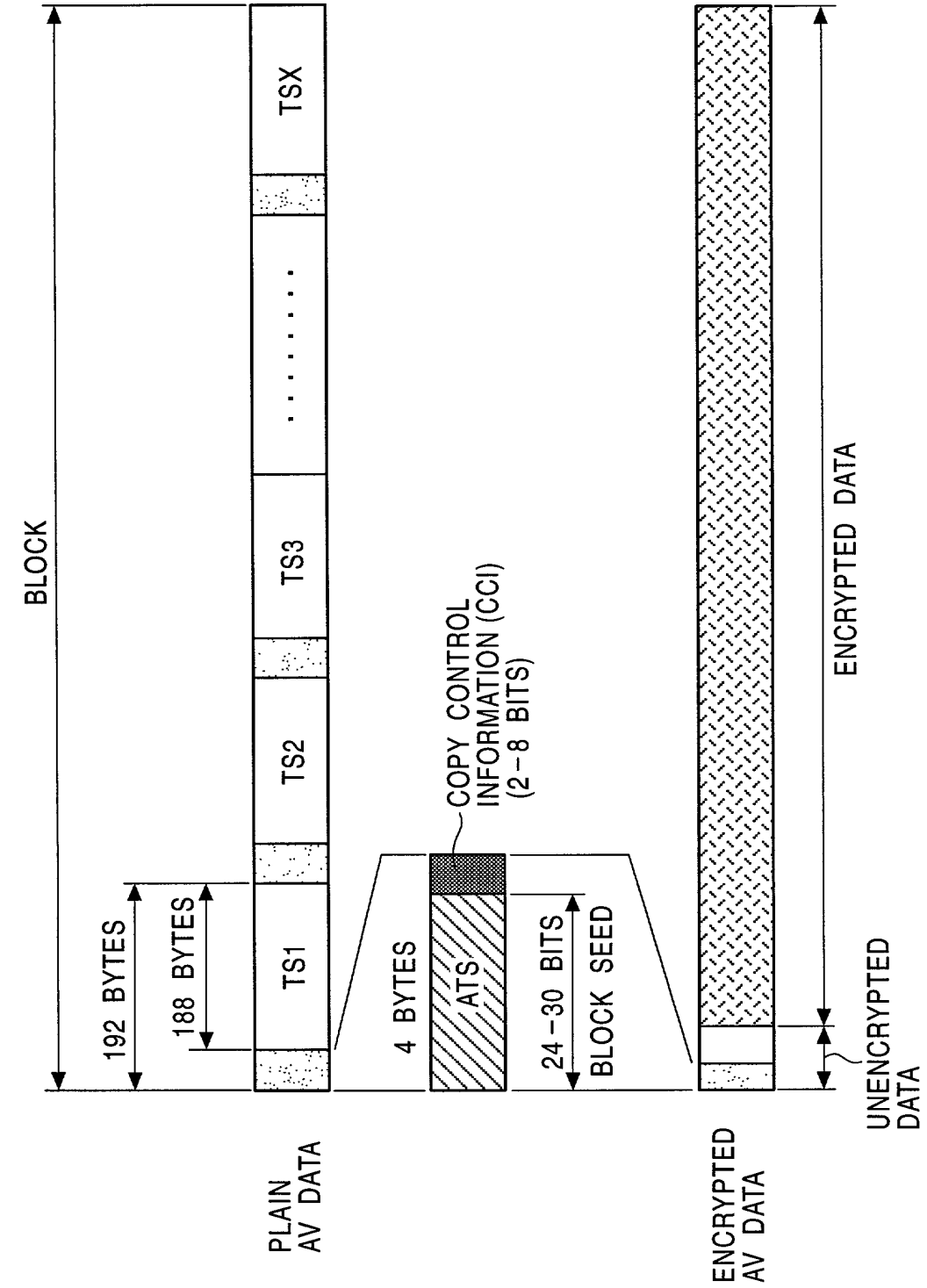
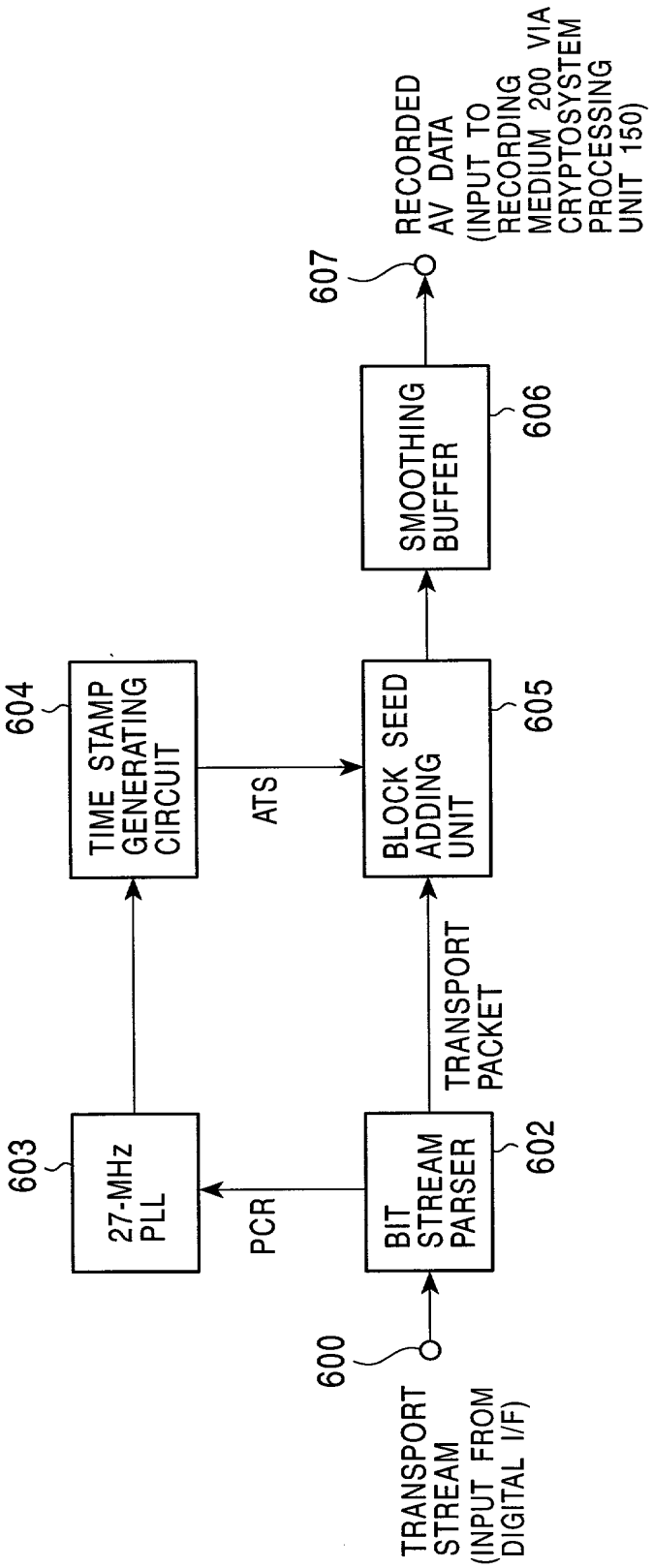

BLOCK
192 BYTES
188 BYTES
TS1
TS2
TS3
TSX
PLAIN AV DATA
4 BYTES
ATS
COPY CONTROL INFORMATION (CCI) (2-8 BITS)
24-30 BITS
BLOCK SEED
ENCRYPTED AV DATA
ENCRYPTED DATA
UNENCRYPTED DATA

FIG. 6


TRANSPORT STREAM (INPUT FROM DIGITAL I/F)
600
BIT STREAM PARSER
602
TRANSPORT PACKET
PCR
27-MHz PLL
603
TIME STAMP GENERATING CIRCUIT
604
ATS
BLOCK SEED ADDING UNIT
605
SMOOTHING BUFFER
606
607
RECORDED AV DATA (INPUT TO RECORDING MEDIUM 200 VIA CRYPTOSYSTEM PROCESSING UNIT 150)

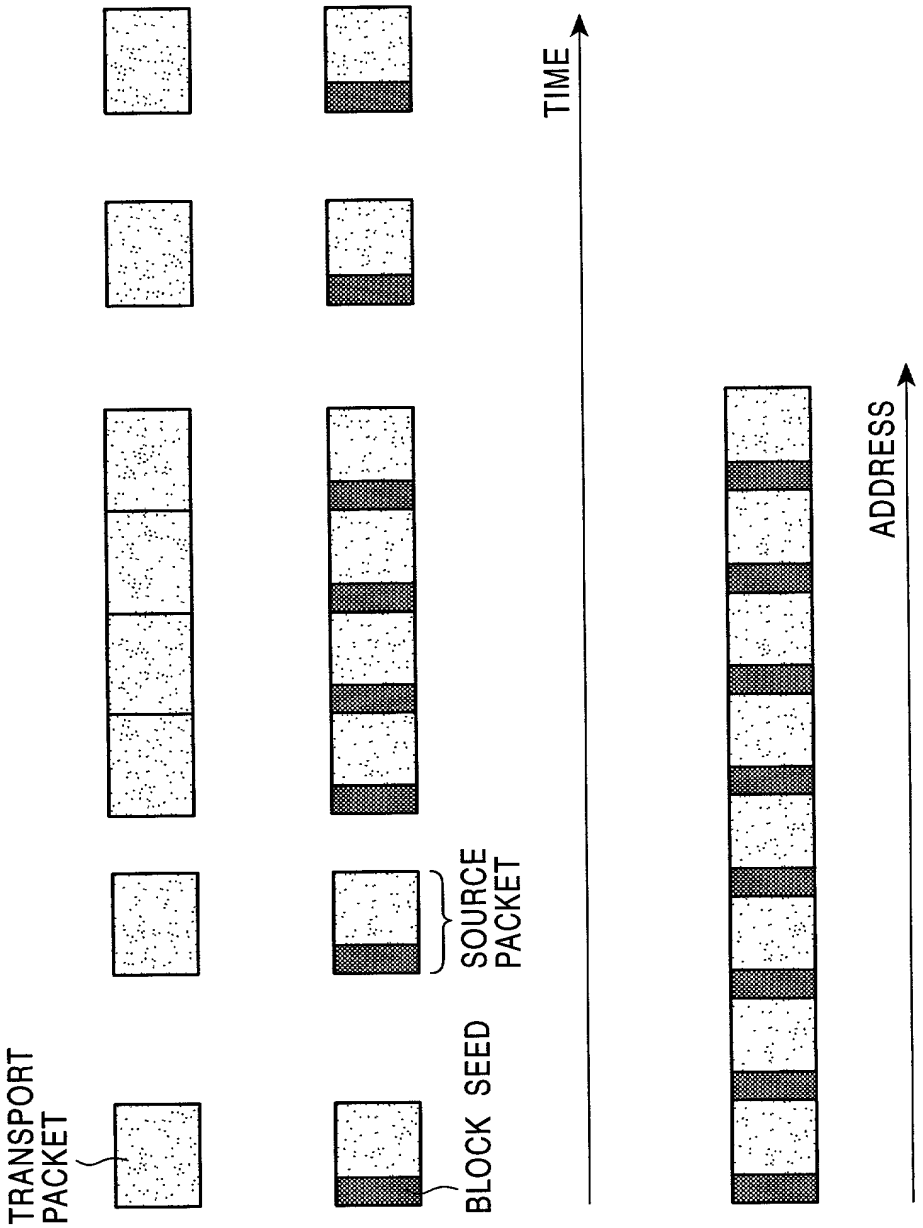


FIG. 7A

FIG. 7B

FIG. 7C

FIG. 8

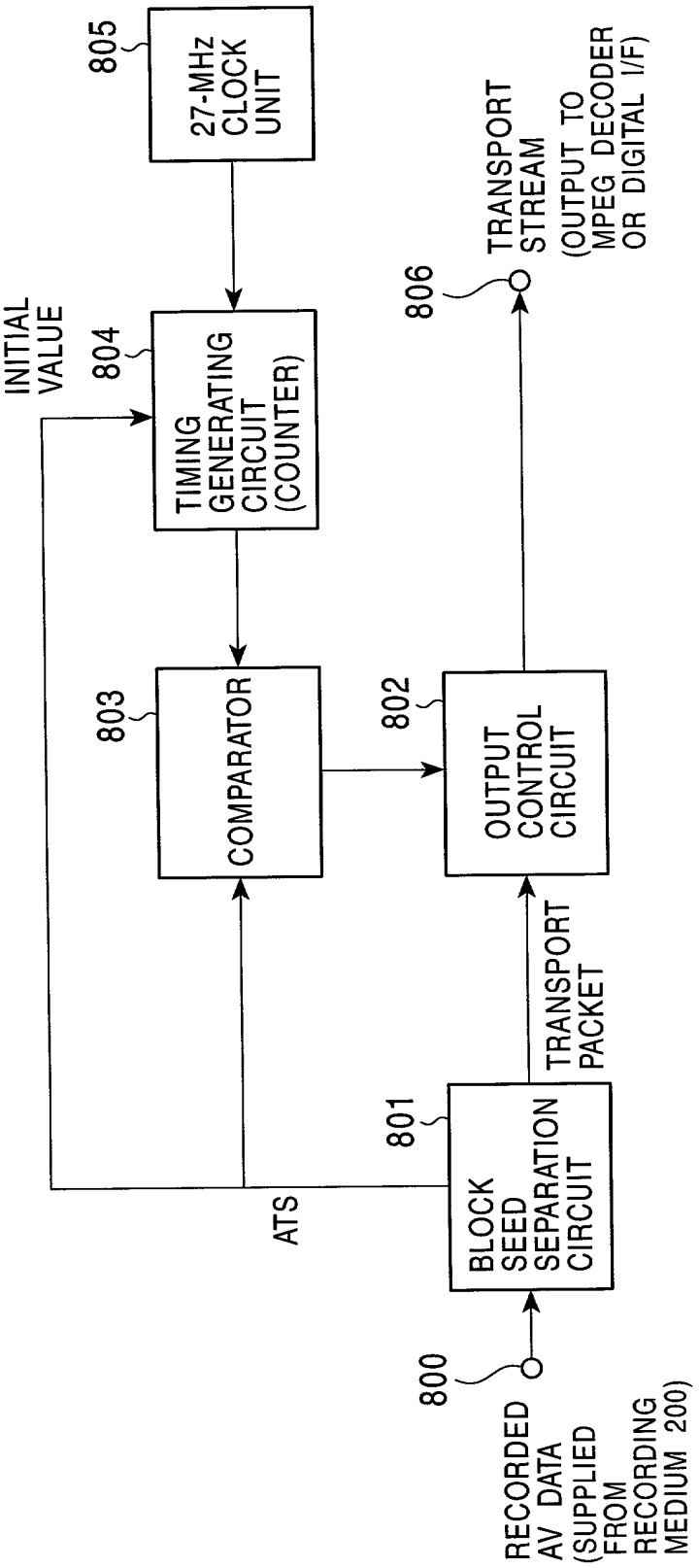

805
27-MHz CLOCK UNIT
INITIAL VALUE
804
TIMING GENERATING CIRCUIT (COUNTER)
806
TRANSPORT STREAM (OUTPUT TO MPEG DECODER OR DIGITAL I/F)
803
COMPARATOR
802
OUTPUT CONTROL CIRCUIT
ATS
801
BLOCK SEED SEPARATION CIRCUIT
TRANSPORT PACKET
800
RECORDED AV DATA (SUPPLIED FROM RECORDING MEDIUM 200)

FIG. 9

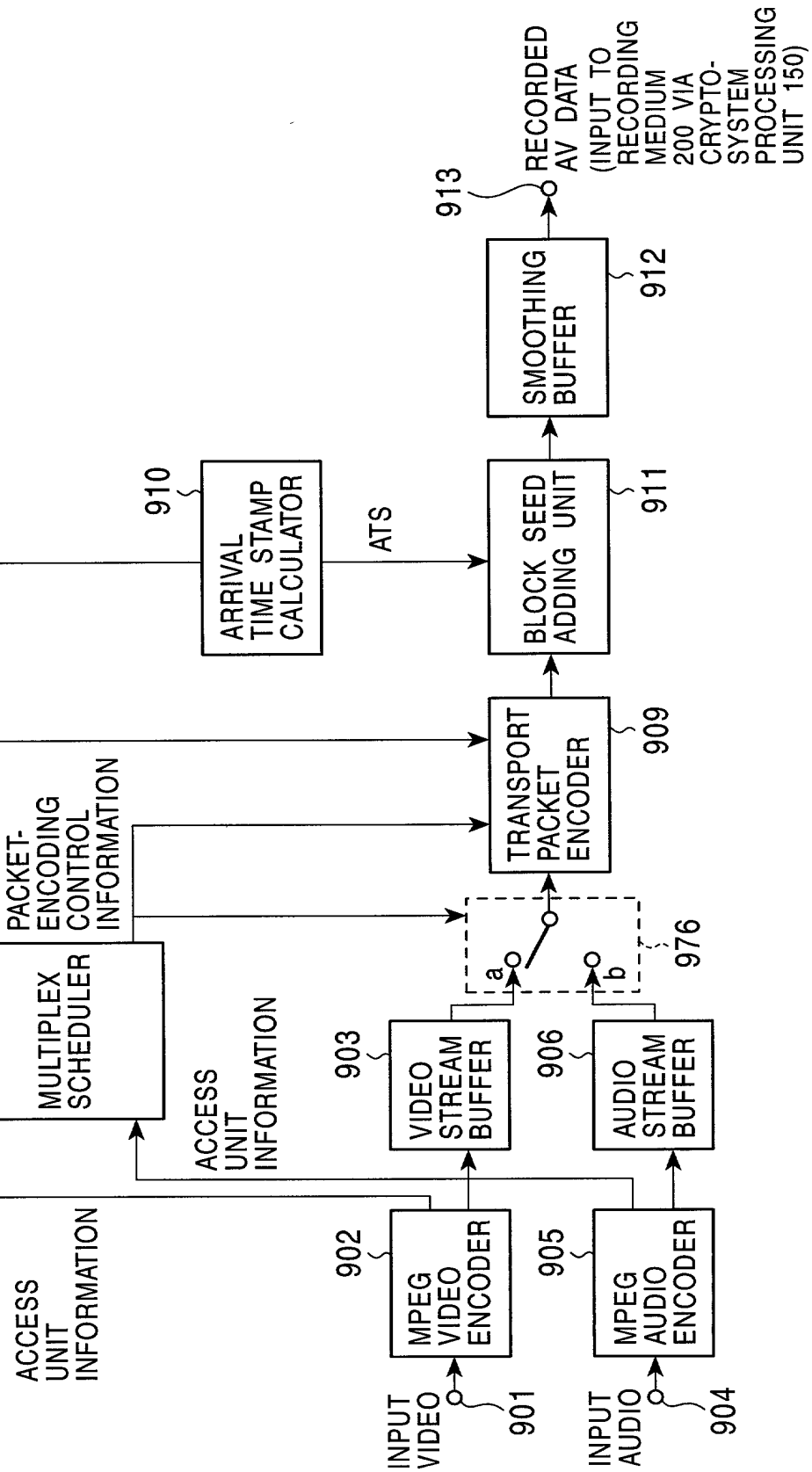

INPUT VIDEO
901
MPEG VIDEO ENCODER
902
INPUT AUDIO
904
MPEG AUDIO ENCODER
905
VIDEO STREAM BUFFER
903
AUDIO STREAM BUFFER
906
a
b
976
ACCESS UNIT INFORMATION
ACCESS UNIT INFORMATION
MULTIPLEX SCHEDULER
908
PACKET-ENCODING CONTROL INFORMATION
TRANSPORT PACKET ENCODER
909
ARRIVAL TIME STAMP CALCULATOR
910
ATS
BLOCK SEED ADDING UNIT
911
SMOOTHING BUFFER
912
913
RECORDED AV DATA
(INPUT TO RECORDING MEDIUM 200 VIA CRYPTO-SYSTEM PROCESSING UNIT 150)

FIG. 10

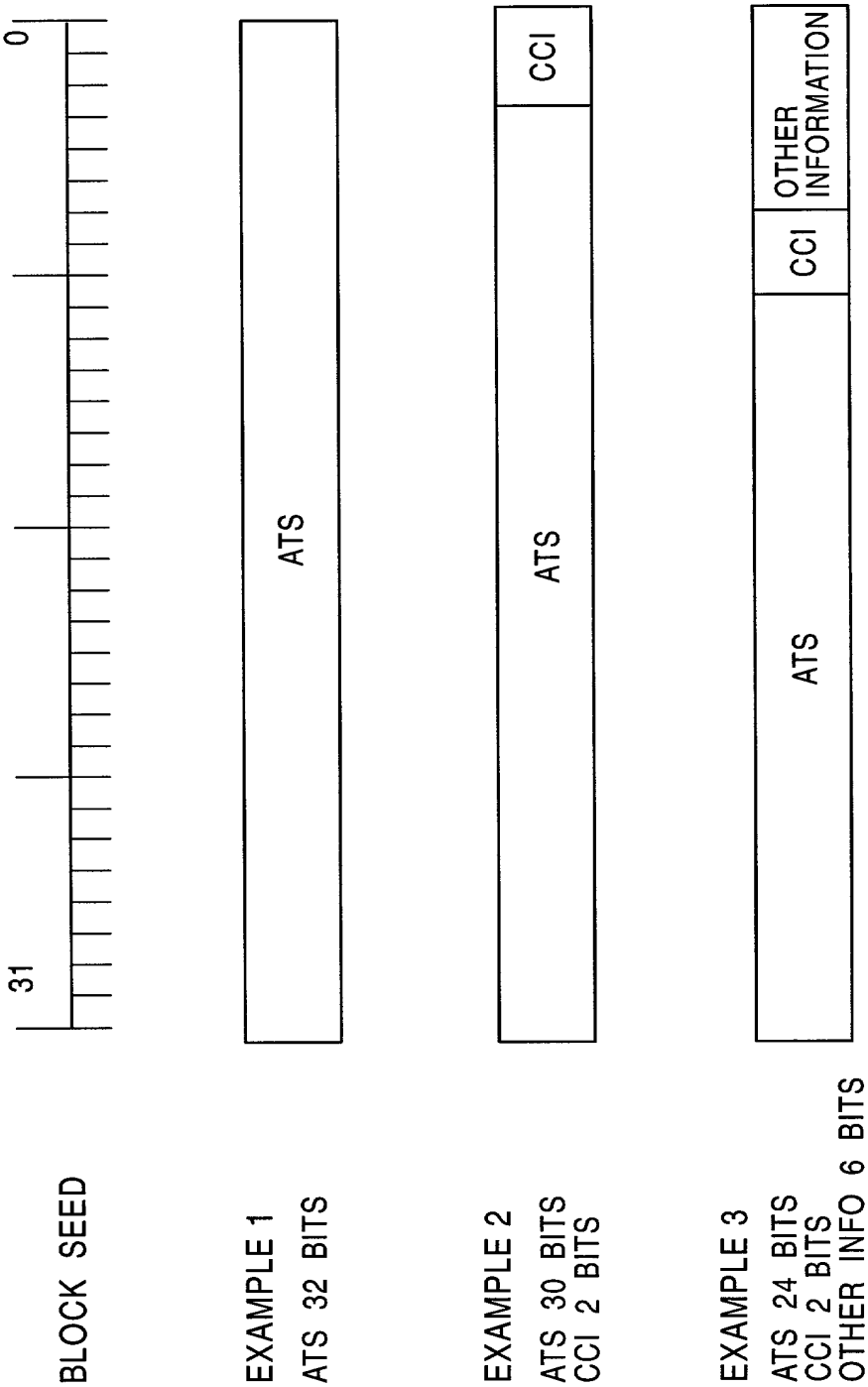

31
0
BLOCK SEED
EXAMPLE 1
ATS 32 BITS
ATS
EXAMPLE 2
ATS 30 BITS
CCI 2 BITS
ATS
CCI
EXAMPLE 3
ATS 24 BITS
CCI 2 BITS
OTHER INFO 6 BITS
ATS
CCI
OTHER INFORMATION

FIG. 11

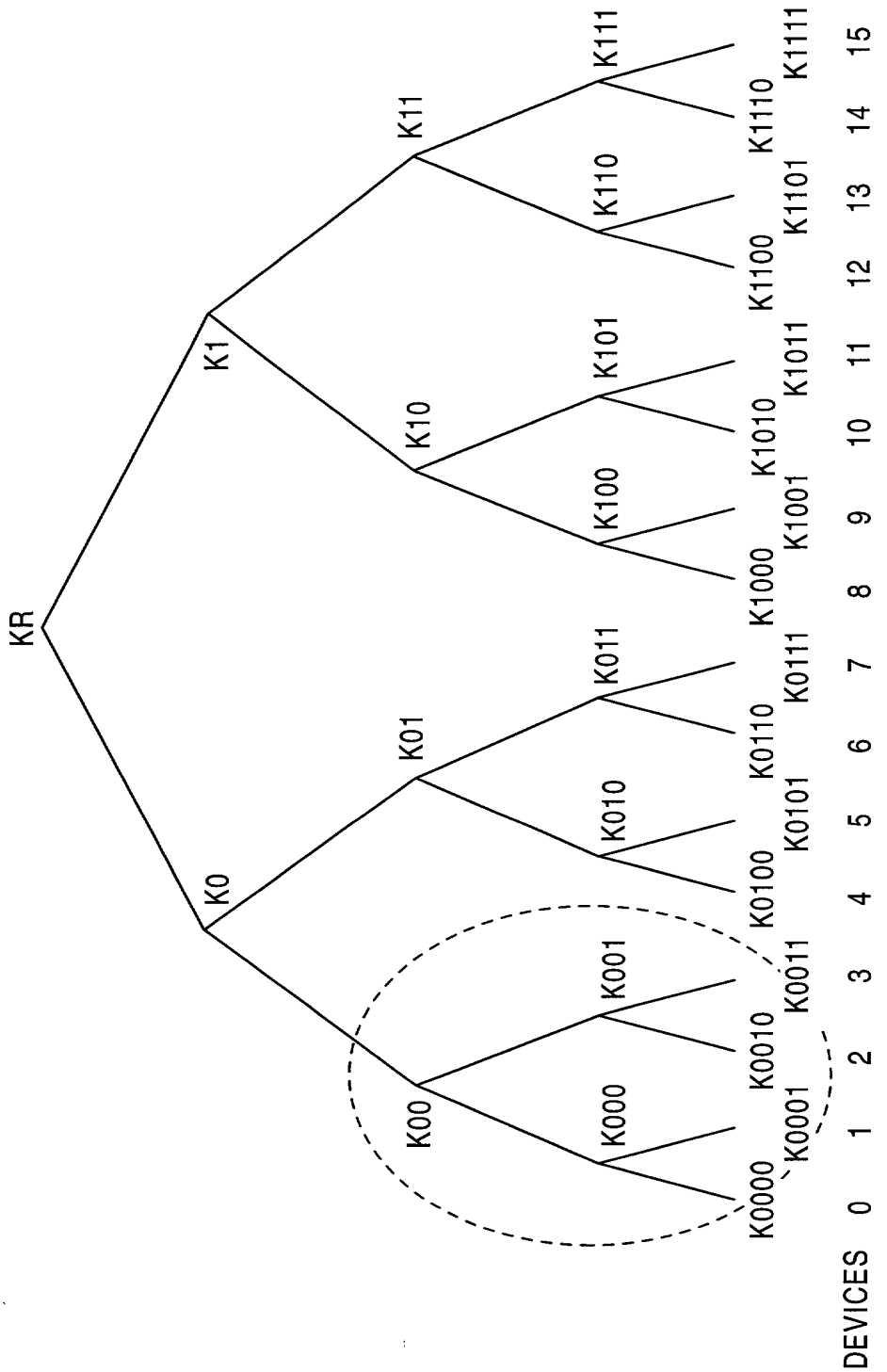

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
DEVICES 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

FIG. 12A

GENERATION: t	
INDEX	ENCRYPTION KEY
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG. 12B

GENERATION: t	
INDEX	ENCRYPTION KEY
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG. 13

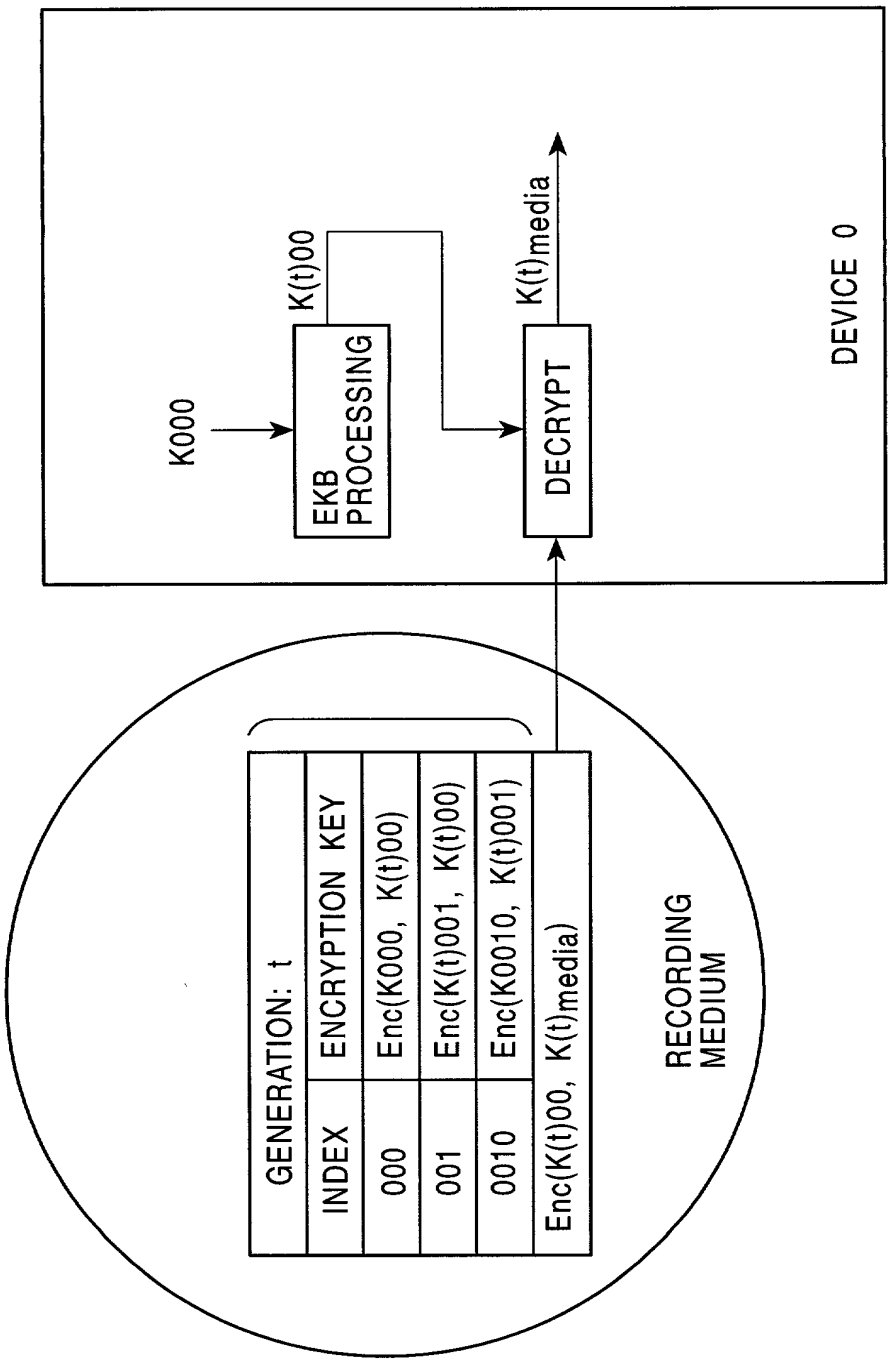

DEVICE 0
K000
EKB PROCESSING
K(t)00
DECRYPT
K(t)media
RECORDING MEDIUM
GENERATION: t
INDEX
ENCRYPTION KEY
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)

FIG. 14

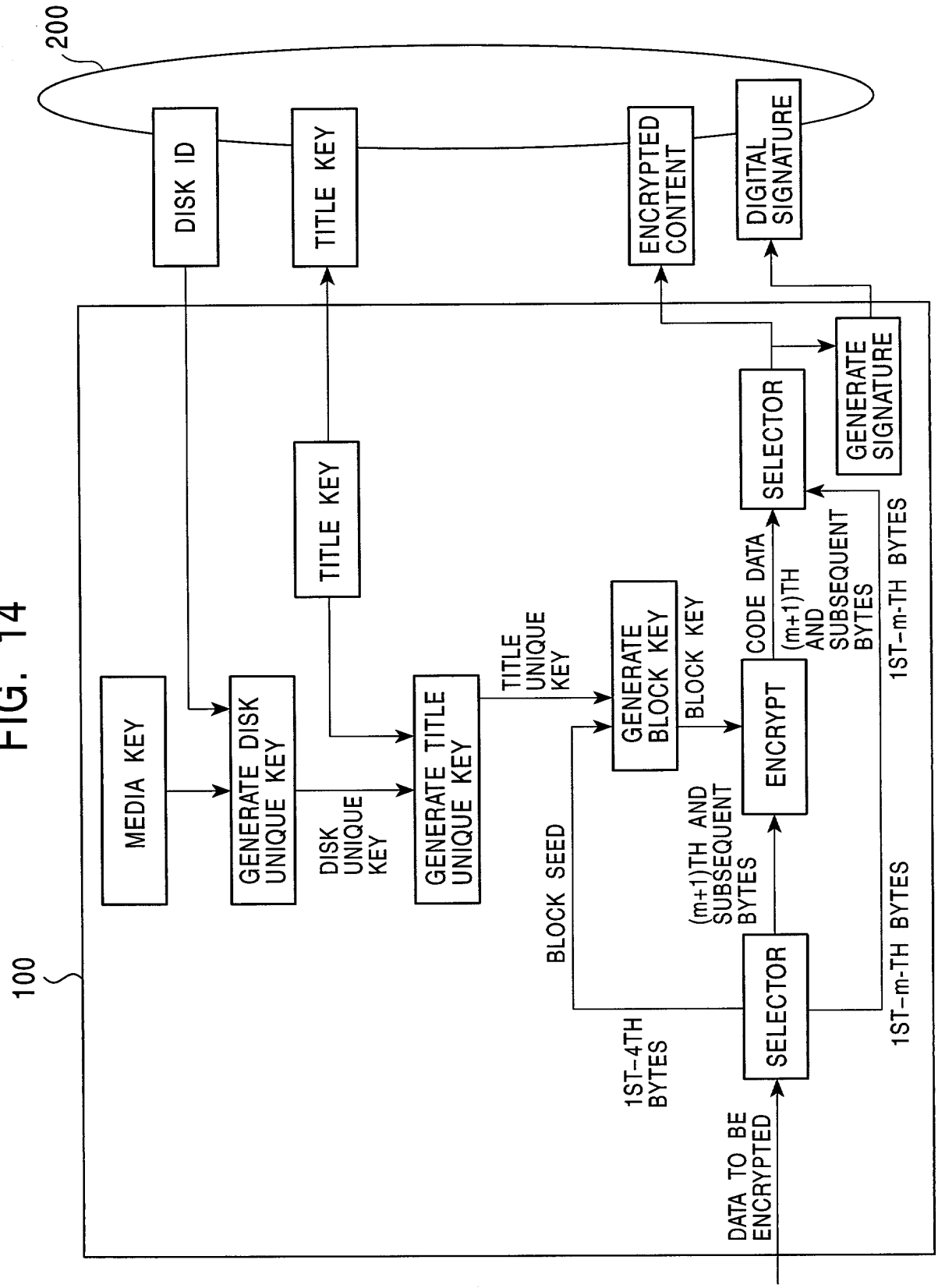

200
DISK ID
TITLE KEY
ENCRYPTED CONTENT
DIGITAL SIGNATURE
100
MEDIA KEY
GENERATE DISK UNIQUE KEY
DISK UNIQUE KEY
TITLE KEY
GENERATE TITLE UNIQUE KEY
TITLE UNIQUE KEY
GENERATE BLOCK KEY
BLOCK KEY
SELECTOR
GENERATE SIGNATURE
CODE DATA
(m+1)TH AND SUBSEQUENT BYTES
1ST-m-TH BYTES
BLOCK SEED
(m+1)TH AND SUBSEQUENT BYTES
ENCRYPT
1ST-4TH BYTES
SELECTOR
1ST-m-TH BYTES
DATA TO BE ENCRYPTED

FIG. 15A

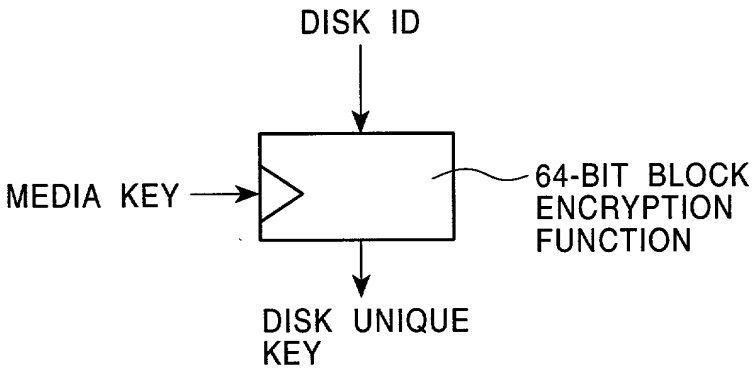


FIG. 15B

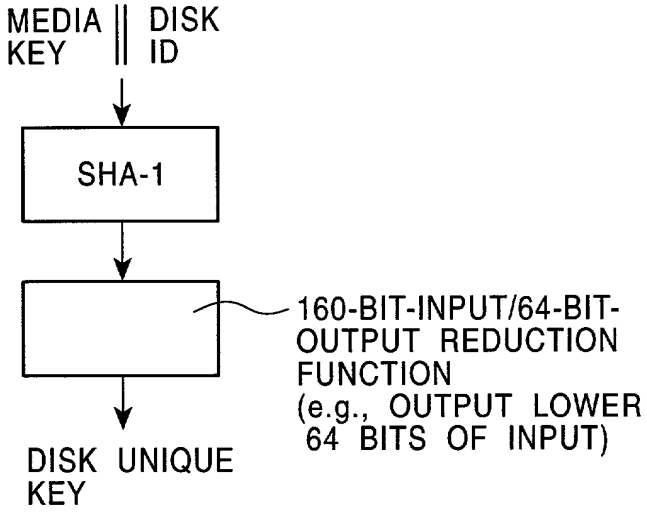


FIG. 16A

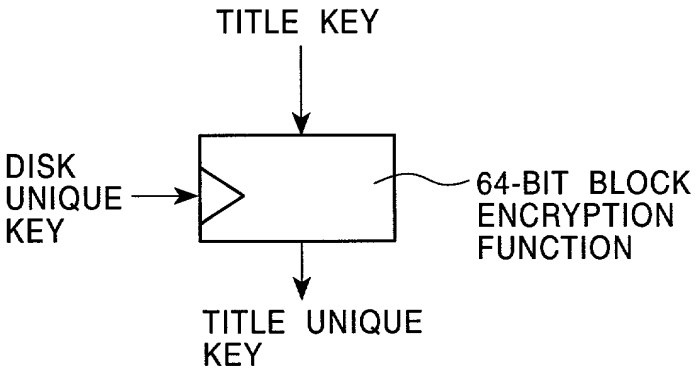


FIG. 16B

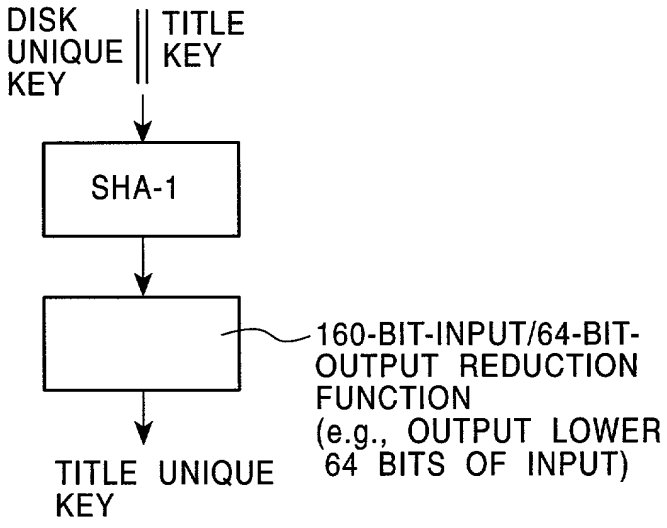


FIG. 17A

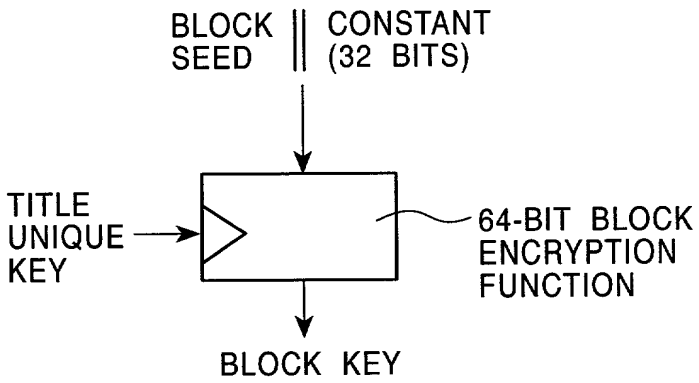


FIG. 17B

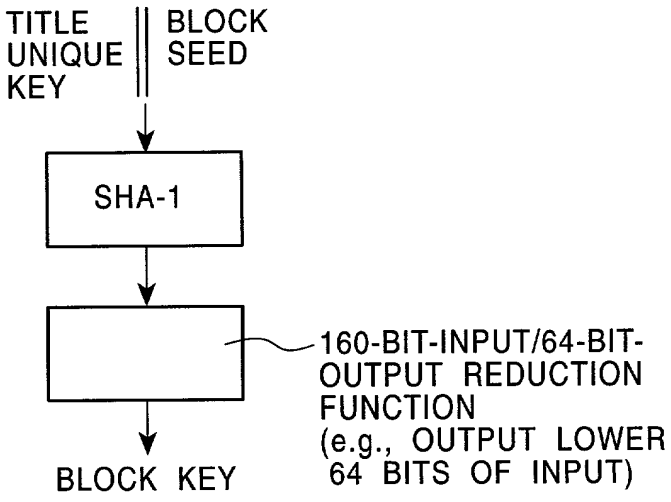


FIG. 18

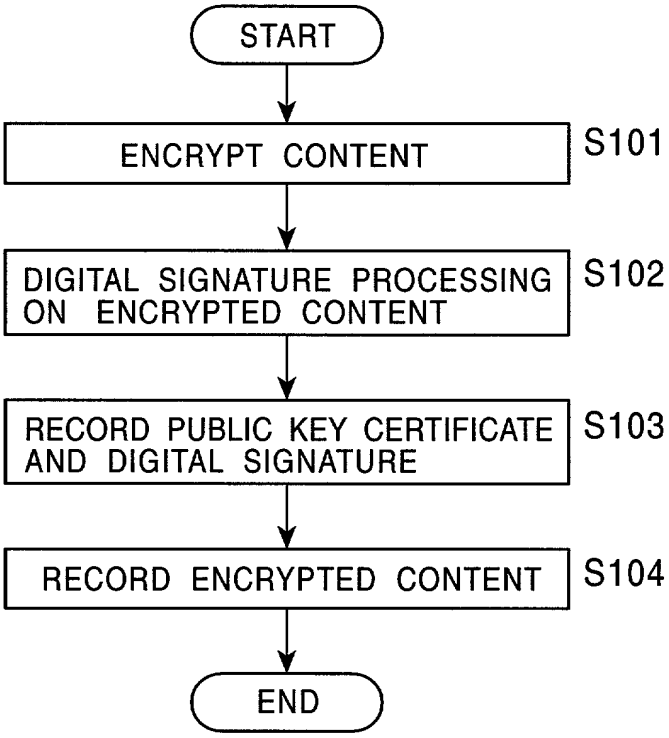

START
ENCRYPT CONTENT
S101
DIGITAL SIGNATURE PROCESSING ON ENCRYPTED CONTENT
S102
RECORD PUBLIC KEY CERTIFICATE AND DIGITAL SIGNATURE
S103
RECORD ENCRYPTED CONTENT
S104
END

FIG. 19

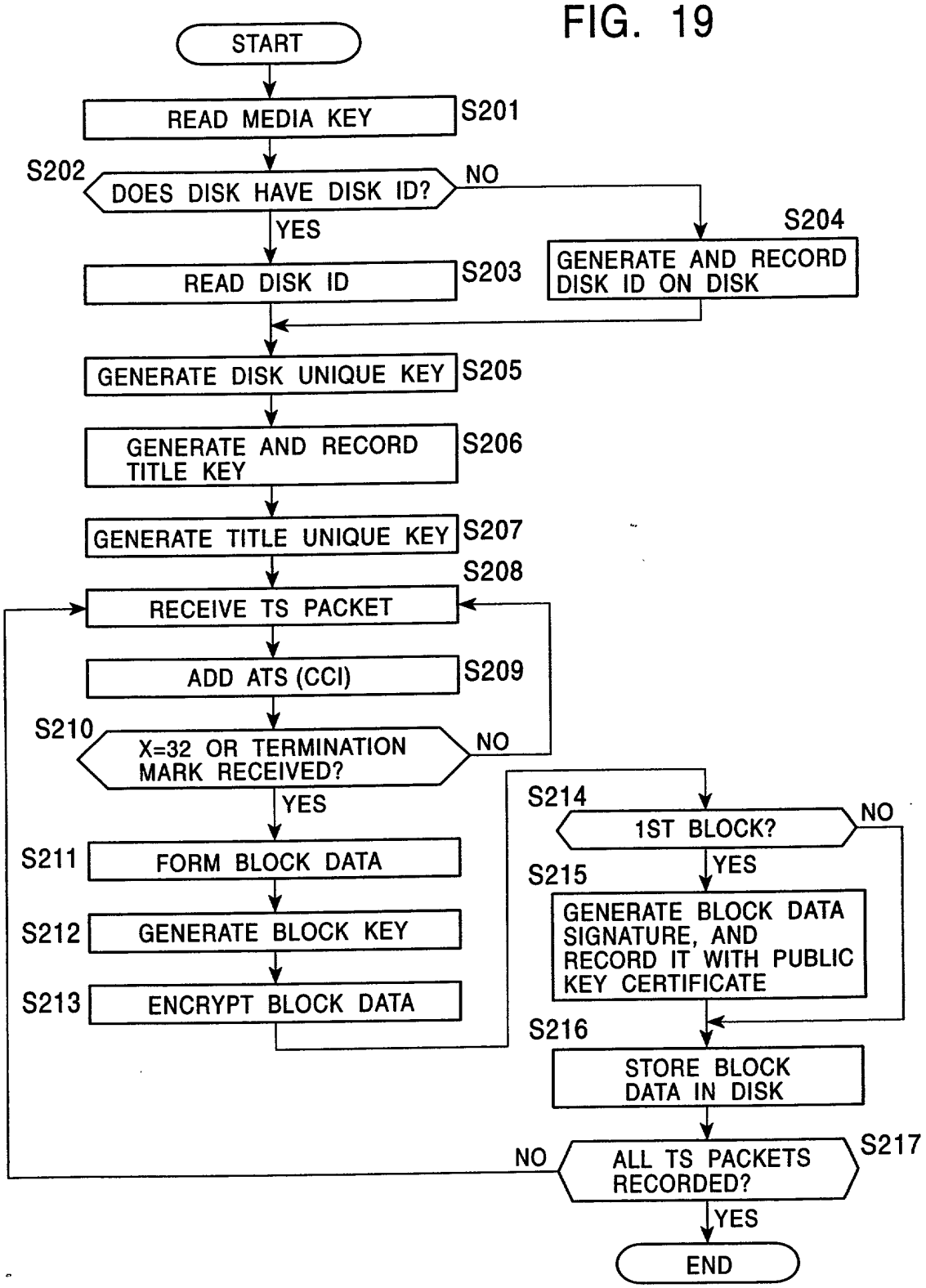

START
READ MEDIA KEY
S201
S202
DOES DISK HAVE DISK ID?
NO
YES
S204
GENERATE AND RECORD DISK ID ON DISK
READ DISK ID
S203
GENERATE DISK UNIQUE KEY
S205
GENERATE AND RECORD TITLE KEY
S206
GENERATE TITLE UNIQUE KEY
S207
S208
RECEIVE TS PACKET
ADD ATS (CCI)
S209
S210
X=32 OR TERMINATION MARK RECEIVED?
NO
YES
S211
FORM BLOCK DATA
S212
GENERATE BLOCK KEY
S213
ENCRYPT BLOCK DATA
S214
1ST BLOCK?
NO
YES
S215
GENERATE BLOCK DATA SIGNATURE, AND RECORD IT WITH PUBLIC KEY CERTIFICATE
S216
STORE BLOCK DATA IN DISK
S217
NO
ALL TS PACKETS RECORDED?
YES
END

FIG. 20

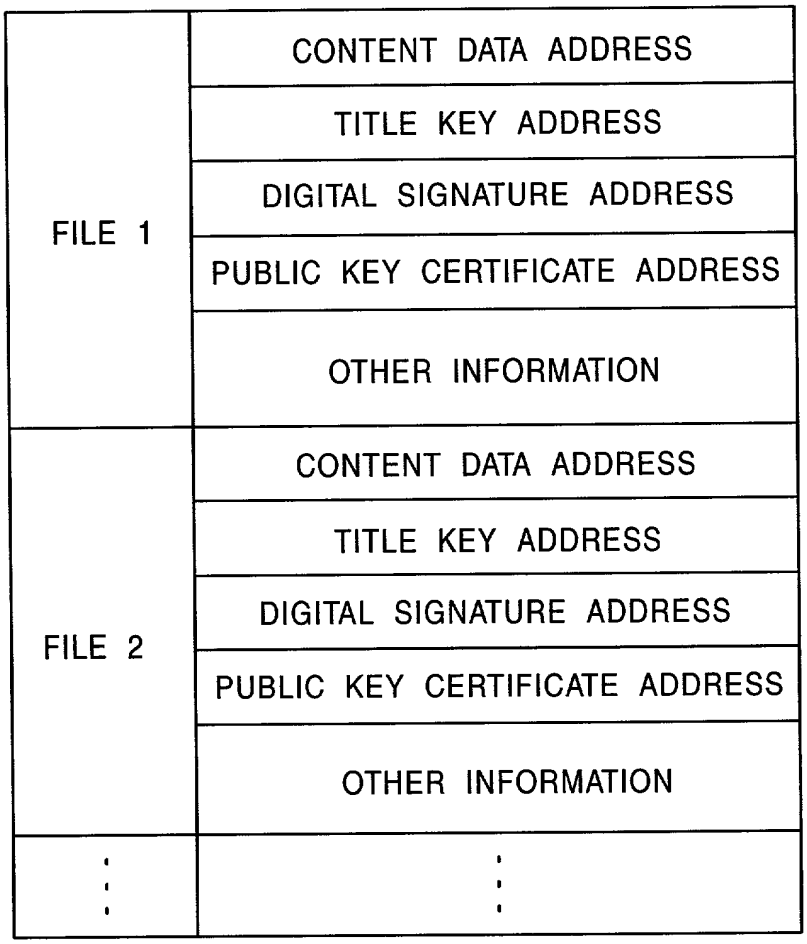

FILE 1
CONTENT DATA ADDRESS
TITLE KEY ADDRESS
DIGITAL SIGNATURE ADDRESS
PUBLIC KEY CERTIFICATE ADDRESS
OTHER INFORMATION
FILE 2
CONTENT DATA ADDRESS
TITLE KEY ADDRESS
DIGITAL SIGNATURE ADDRESS
PUBLIC KEY CERTIFICATE ADDRESS
OTHER INFORMATION

FIG. 21

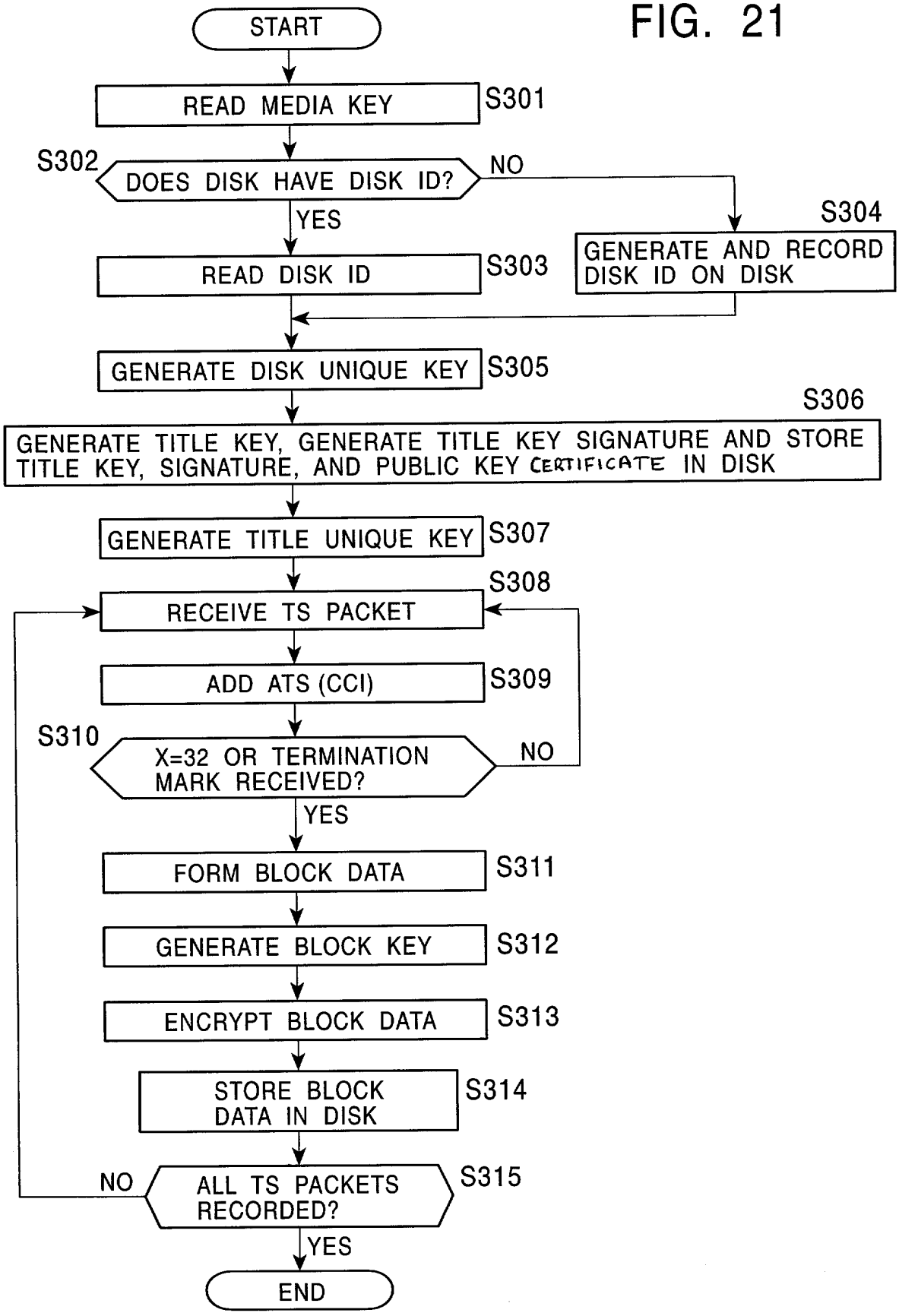

START
READ MEDIA KEY
S301
S302
DOES DISK HAVE DISK ID?
NO
YES
S304
GENERATE AND RECORD DISK ID ON DISK
READ DISK ID
S303
GENERATE DISK UNIQUE KEY
S305
S306
GENERATE TITLE KEY, GENERATE TITLE KEY SIGNATURE AND STORE TITLE KEY, SIGNATURE, AND PUBLIC KEY CERTIFICATE IN DISK
GENERATE TITLE UNIQUE KEY
S307
S308
RECEIVE TS PACKET
ADD ATS (CCI)
S309
S310
X=32 OR TERMINATION MARK RECEIVED?
NO
YES
FORM BLOCK DATA
S311
GENERATE BLOCK KEY
S312
ENCRYPT BLOCK DATA
S313
STORE BLOCK DATA IN DISK
S314
NO
ALL TS PACKETS RECORDED?
S315
YES
END

FIG. 22

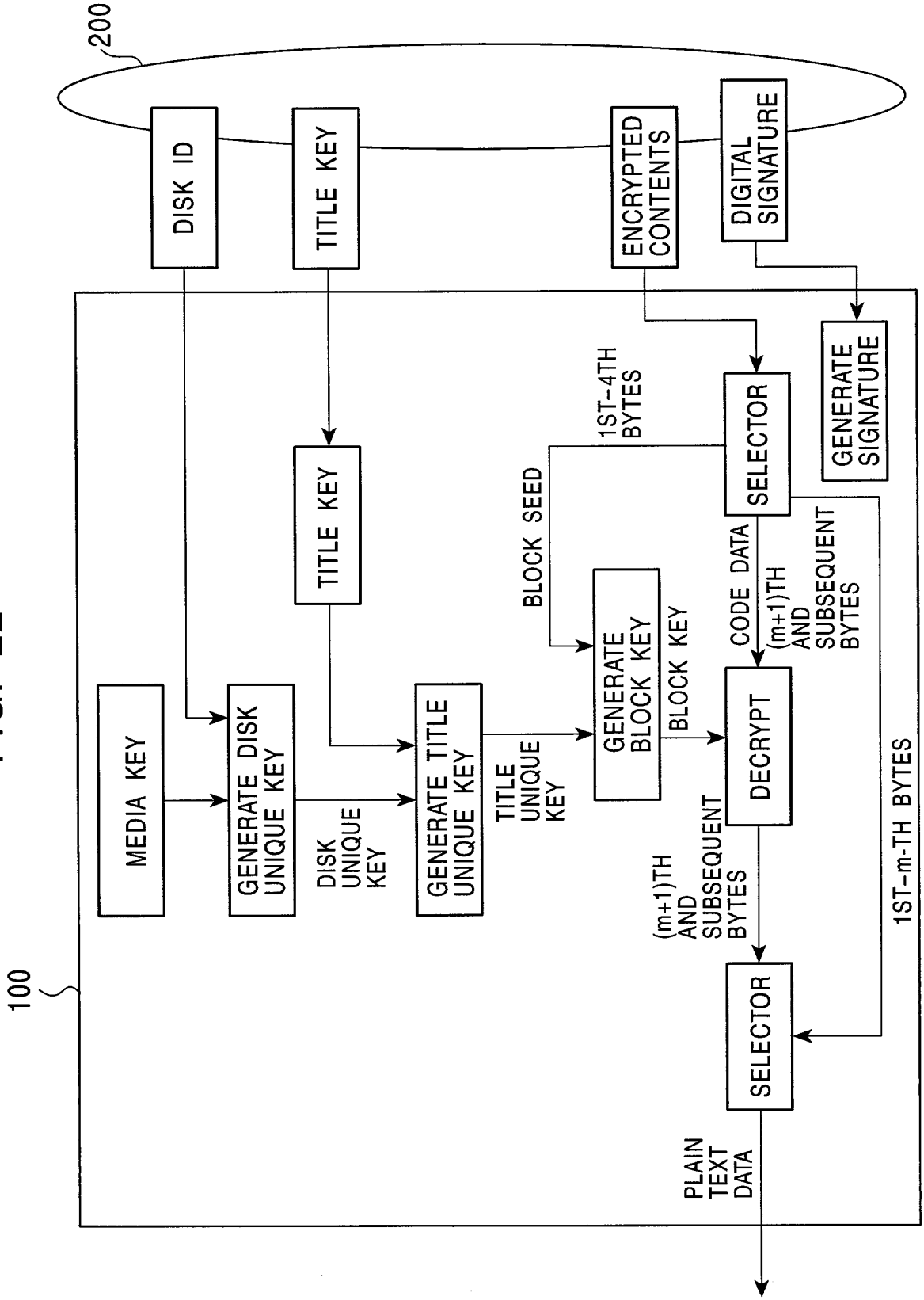

200
DISK ID
TITLE KEY
ENCRYPTED CONTENTS
DIGITAL SIGNATURE
100
MEDIA KEY
GENERATE DISK UNIQUE KEY
DISK UNIQUE KEY
TITLE KEY
GENERATE TITLE UNIQUE KEY
TITLE UNIQUE KEY
BLOCK SEED
1ST-4TH BYTES
SELECTOR
GENERATE SIGNATURE
GENERATE BLOCK KEY
BLOCK KEY
CODE DATA
(m+1)TH AND SUBSEQUENT BYTES
DECRYPT
(m+1)TH AND SUBSEQUENT BYTES
1ST-m-TH BYTES
SELECTOR
PLAIN TEXT DATA

FIG. 23

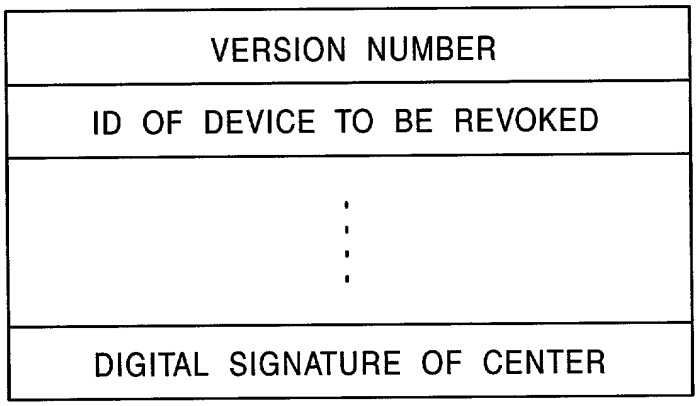

VERSION NUMBER
ID OF DEVICE TO BE REVOKED
DIGITAL SIGNATURE OF CENTER

FIG. 24

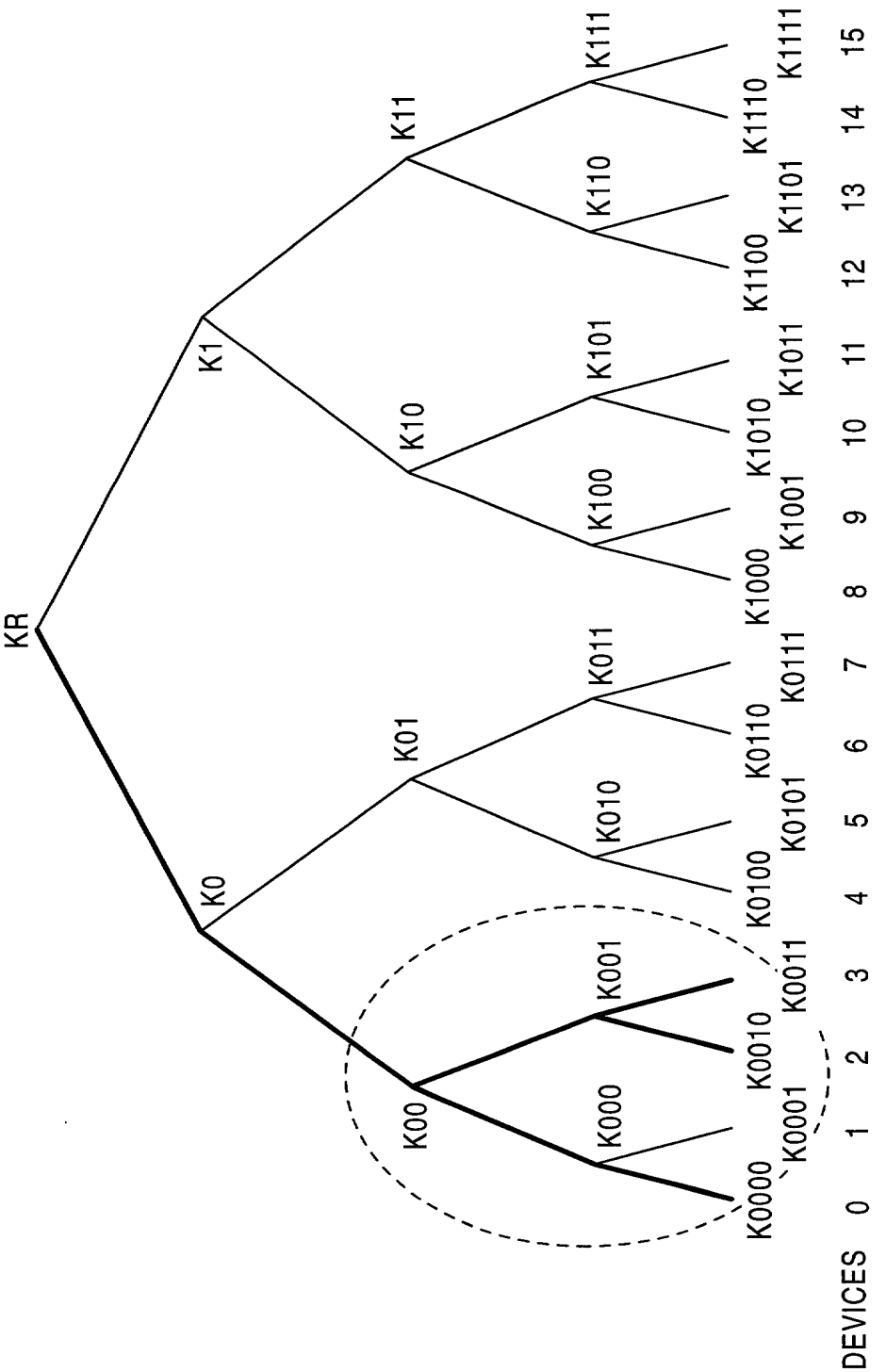

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
DEVICES 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

FIG. 25

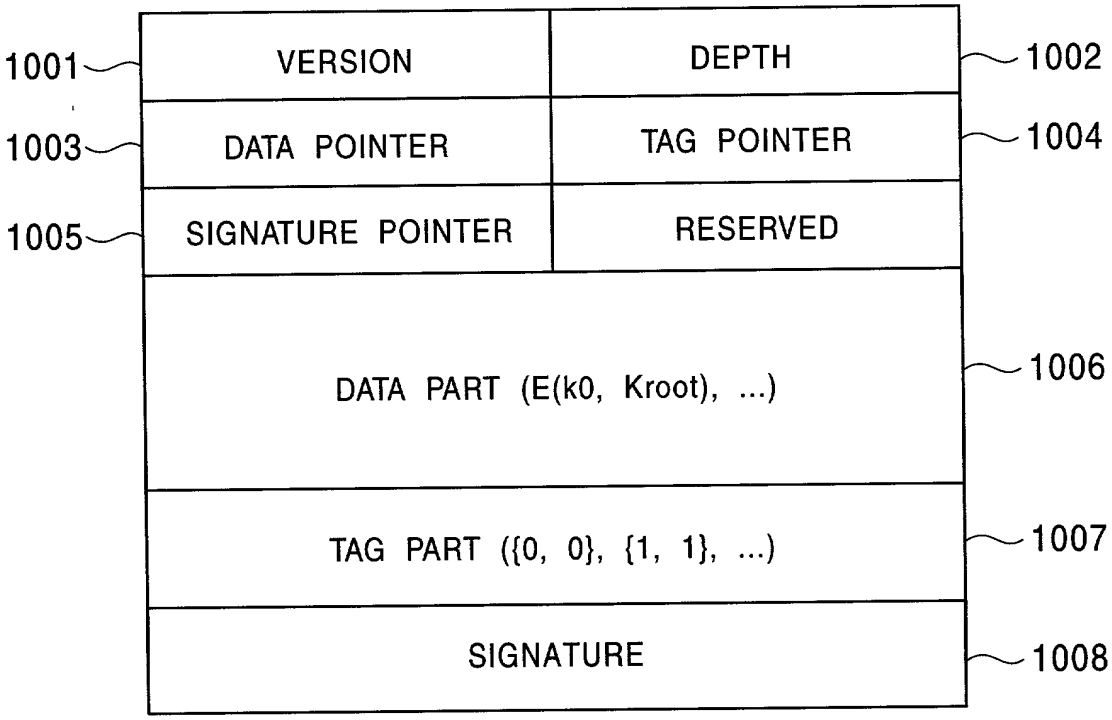

1001
VERSION
DEPTH
1002
1003
DATA POINTER
TAG POINTER
1004
1005
SIGNATURE POINTER
RESERVED
DATA PART (E(k0, Kroot), ...)
1006
TAG PART ({0, 0}, {1, 1}, ...)
1007
SIGNATURE
1008

FIG. 26

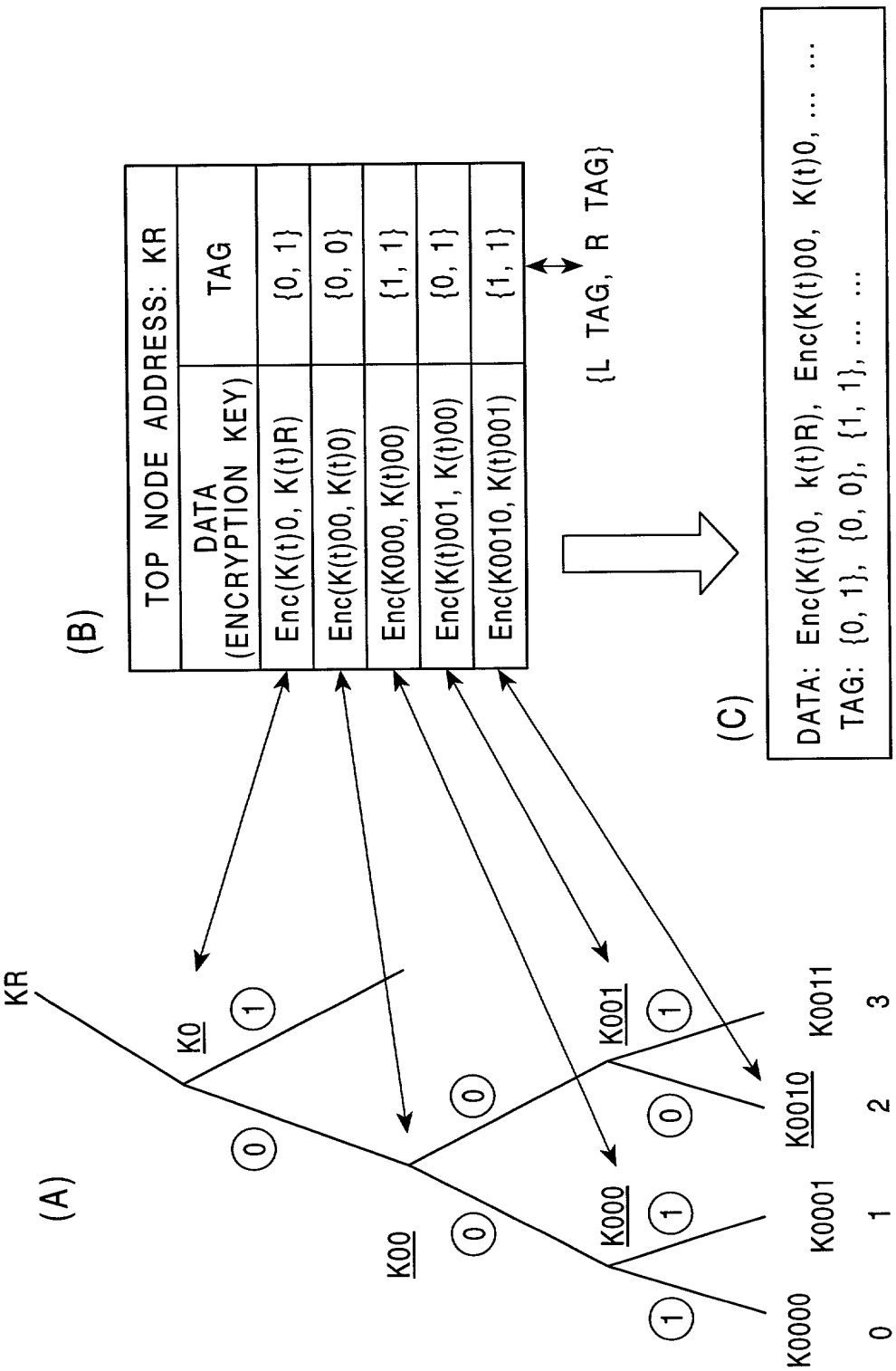

(A)
KR
K0
K00
K000
K001
K0000
K0001
K0010
K0011
0
1
2
3
(B)
TOP NODE ADDRESS: KR
DATA (ENCRYPTION KEY)
TAG
Enc(K(t)0, K(t)R)
{0, 1}
Enc(K(t)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(t)001, K(t)00)
{0, 1}
Enc(K0010, K(t)001)
{1, 1}
{L TAG, R TAG}
(C)
DATA: Enc(K(t)0, k(t)R), Enc(K(t)00, K(t)0, ...
TAG: {0, 1}, {0, 0}, {1, 1}, ...

FIG. 27A

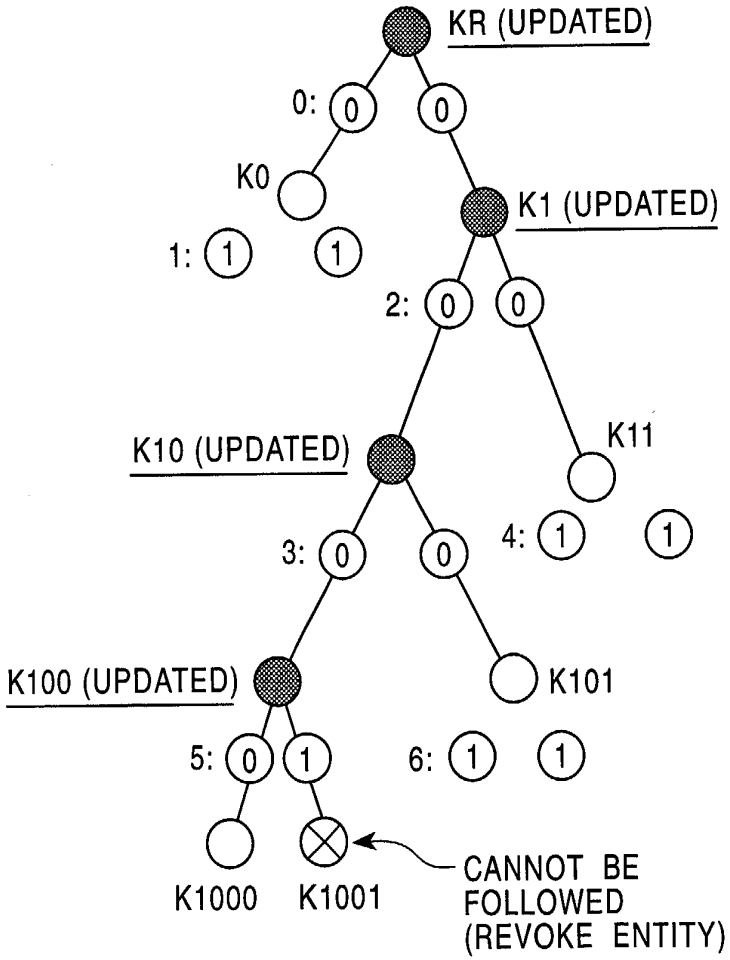


FIG. 27B

DATA (ENCRYPTION KEY)	Enc(K0, K(t)R), Enc(K(t)1, K(t)R) Enc(K(t)10, K(t)1), Enc(K11, K(t)1) Enc(K(t)100, K(t)10), Enc(K101, K(t)10) Enc(K1000, K(t)100)
TAG	0: {0, 0}, 1: {1, 1}, 2: {0, 0}, 3: {0, 0}, 4: {1, 1}, 5: {0, 1}, 6: {1, 1},

{L TAG, R TAG}

FIG. 28A

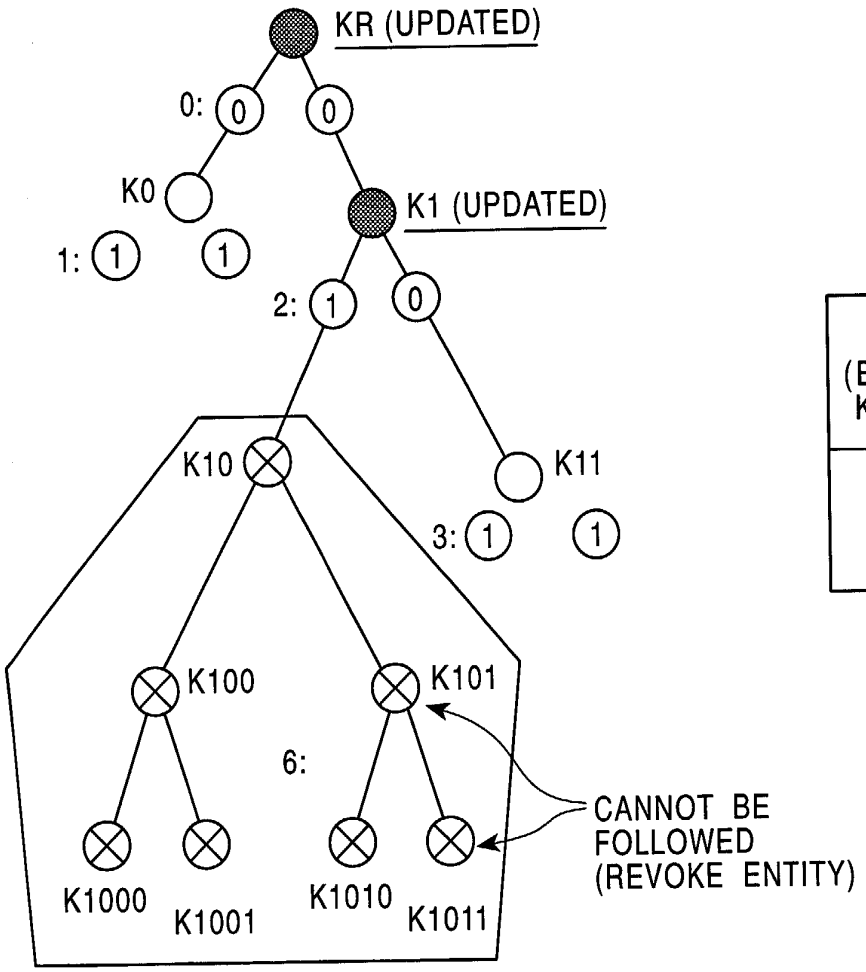


FIG. 28B

DATA (ENCRYPTION KEY)	Enc(K0, K(t)R), Enc(K(t)1, K(t)R) Enc(K11, K(t)1)
TAG	0: {0, 0}, 1: {1, 1}, 2: {1, 0}, 3: {1, 1}

{L TAG, R TAG}

FIG. 29

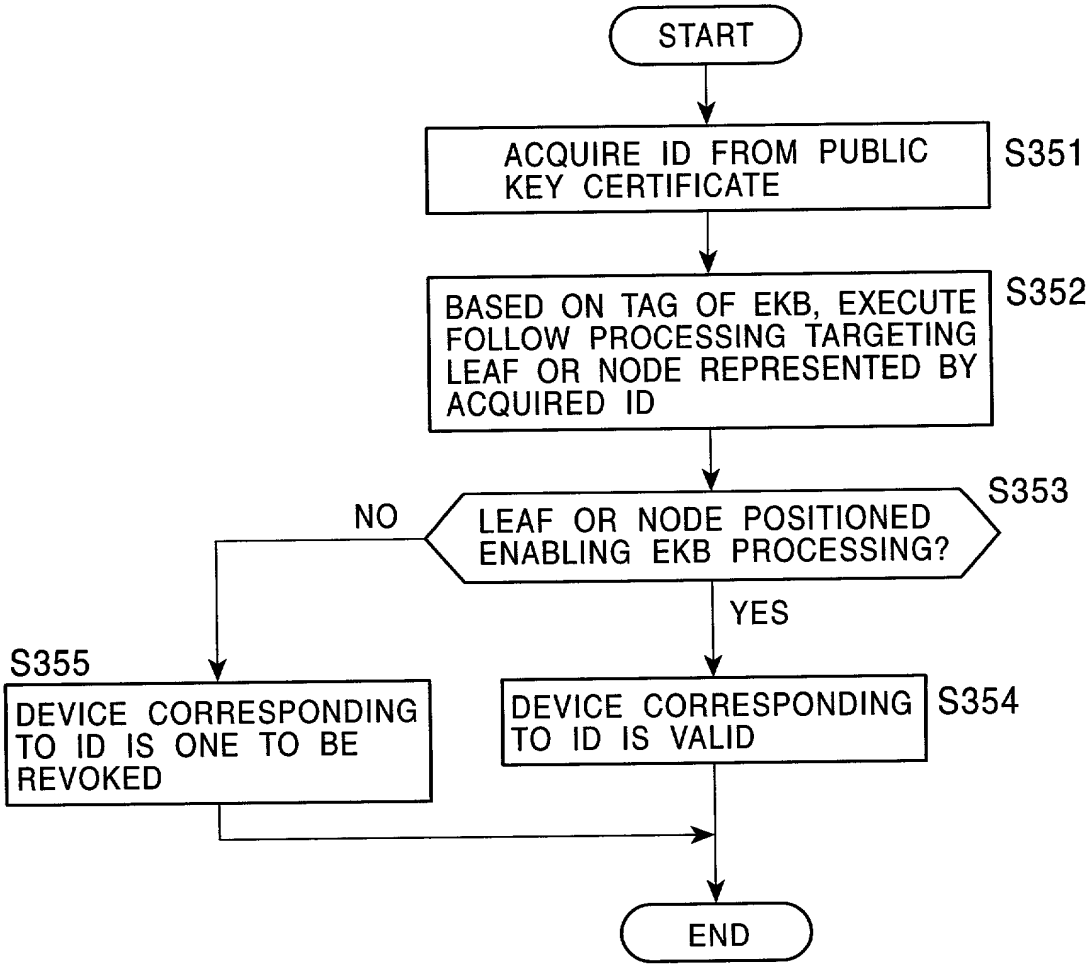

START
ACQUIRE ID FROM PUBLIC KEY CERTIFICATE
S351
BASED ON TAG OF EKB, EXECUTE FOLLOW PROCESSING TARGETING LEAF OR NODE REPRESENTED BY ACQUIRED ID
S352
LEAF OR NODE POSITIONED ENABLING EKB PROCESSING?
S353
NO
YES
DEVICE CORRESPONDING TO ID IS ONE TO BE REVOKED
S355
DEVICE CORRESPONDING TO ID IS VALID
S354
END

FIG. 30

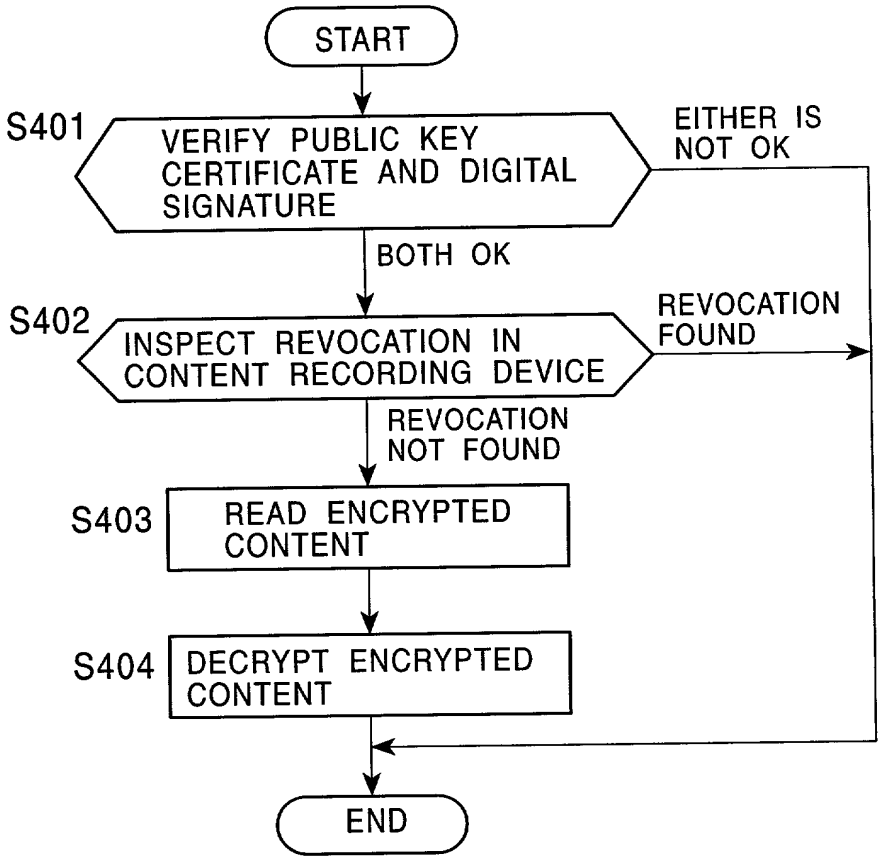

START
S401
VERIFY PUBLIC KEY CERTIFICATE AND DIGITAL SIGNATURE
EITHER IS NOT OK
BOTH OK
S402
INSPECT REVOCATION IN CONTENT RECORDING DEVICE
REVOCATION FOUND
REVOCATION NOT FOUND
S403
READ ENCRYPTED CONTENT
S404
DECRYPT ENCRYPTED CONTENT
END

FIG. 31

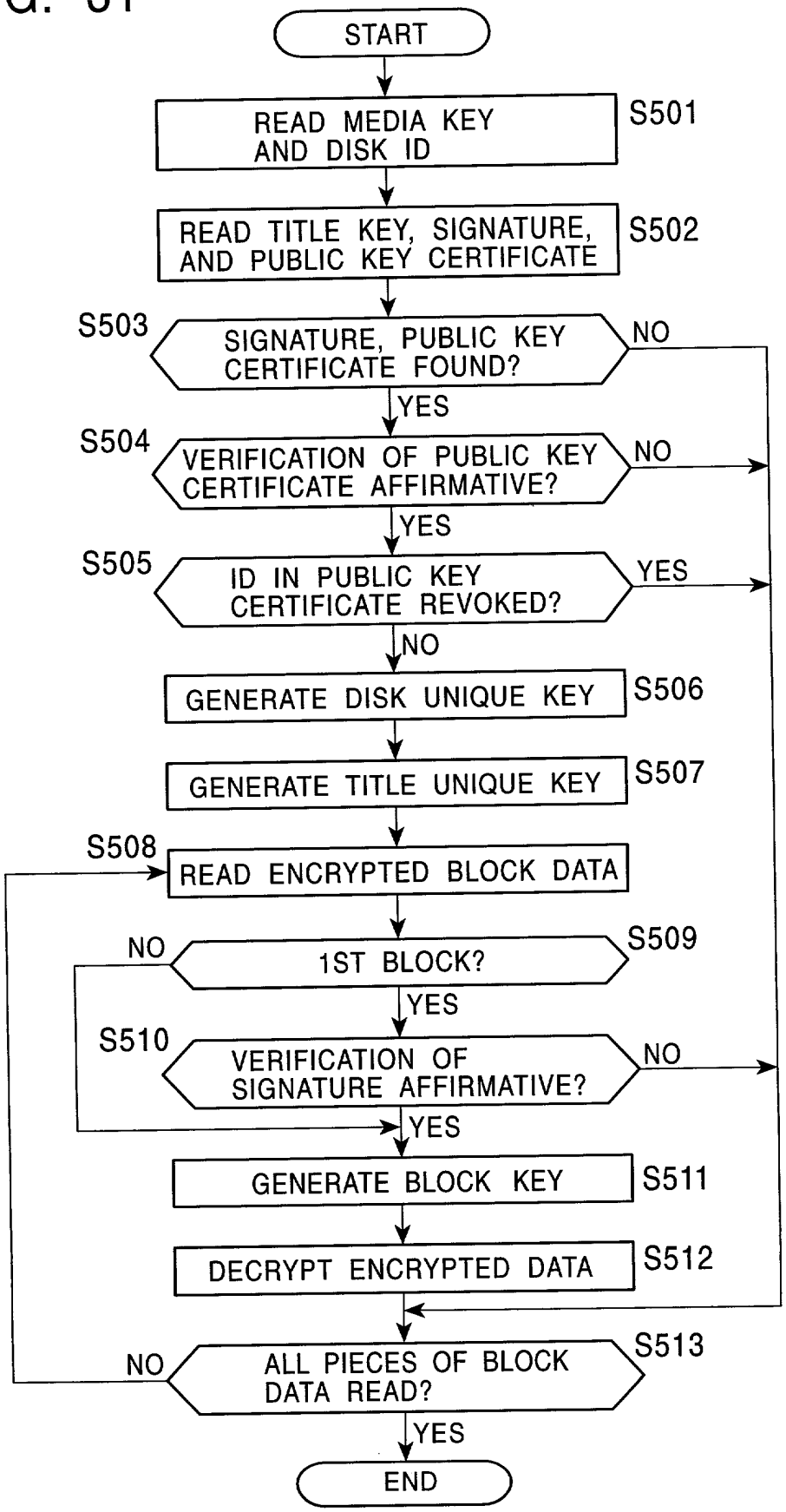

START
READ MEDIA KEY AND DISK ID
S501
READ TITLE KEY, SIGNATURE, AND PUBLIC KEY CERTIFICATE
S502
S503
SIGNATURE, PUBLIC KEY CERTIFICATE FOUND?
NO
YES
S504
VERIFICATION OF PUBLIC KEY CERTIFICATE AFFIRMATIVE?
NO
YES
S505
ID IN PUBLIC KEY CERTIFICATE REVOKED?
YES
NO
GENERATE DISK UNIQUE KEY
S506
GENERATE TITLE UNIQUE KEY
S507
S508
READ ENCRYPTED BLOCK DATA
NO
1ST BLOCK?
S509
YES
S510
VERIFICATION OF SIGNATURE AFFIRMATIVE?
NO
YES
GENERATE BLOCK KEY
S511
DECRYPT ENCRYPTED DATA
S512
NO
ALL PIECES OF BLOCK DATA READ?
S513
YES
END

FIG. 32

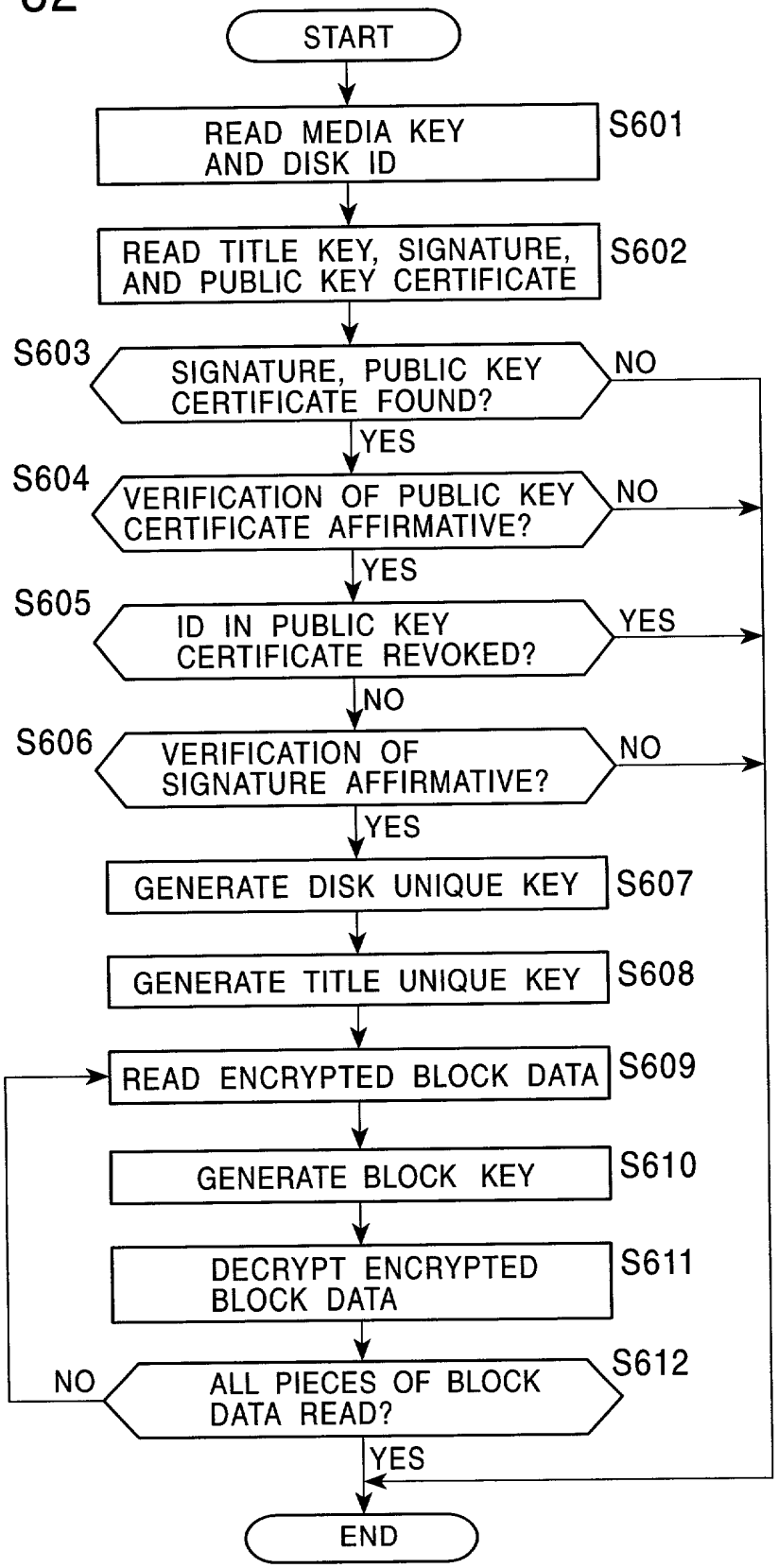

START
READ MEDIA KEY AND DISK ID
S601
READ TITLE KEY, SIGNATURE, AND PUBLIC KEY CERTIFICATE
S602
S603
SIGNATURE, PUBLIC KEY CERTIFICATE FOUND?
NO
YES
S604
VERIFICATION OF PUBLIC KEY CERTIFICATE AFFIRMATIVE?
NO
YES
S605
ID IN PUBLIC KEY CERTIFICATE REVOKED?
YES
NO
S606
VERIFICATION OF SIGNATURE AFFIRMATIVE?
NO
YES
GENERATE DISK UNIQUE KEY
S607
GENERATE TITLE UNIQUE KEY
S608
READ ENCRYPTED BLOCK DATA
S609
GENERATE BLOCK KEY
S610
DECRYPT ENCRYPTED BLOCK DATA
S611
S612
NO
ALL PIECES OF BLOCK DATA READ?
YES
END

FIG. 33A

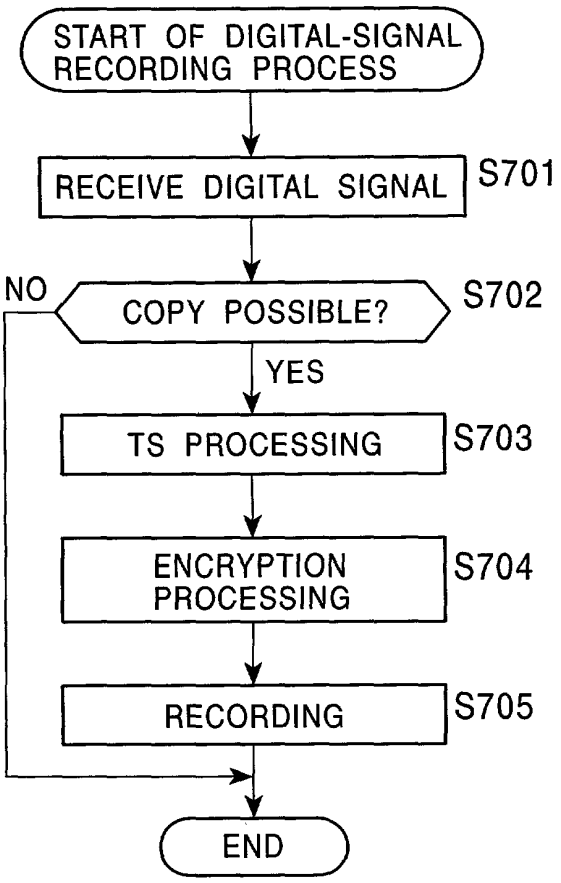


FIG. 33B

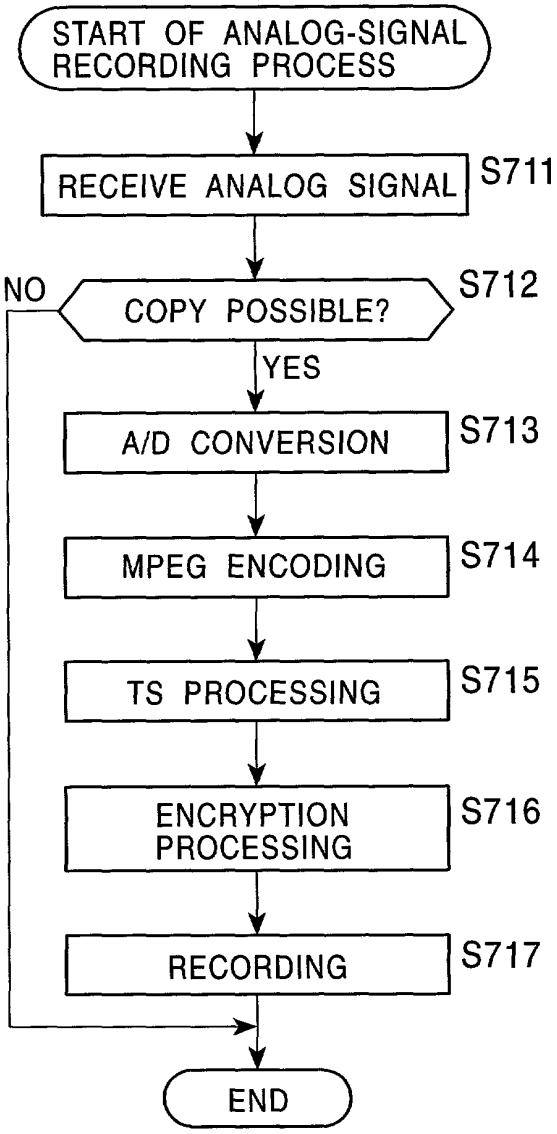


FIG. 34A

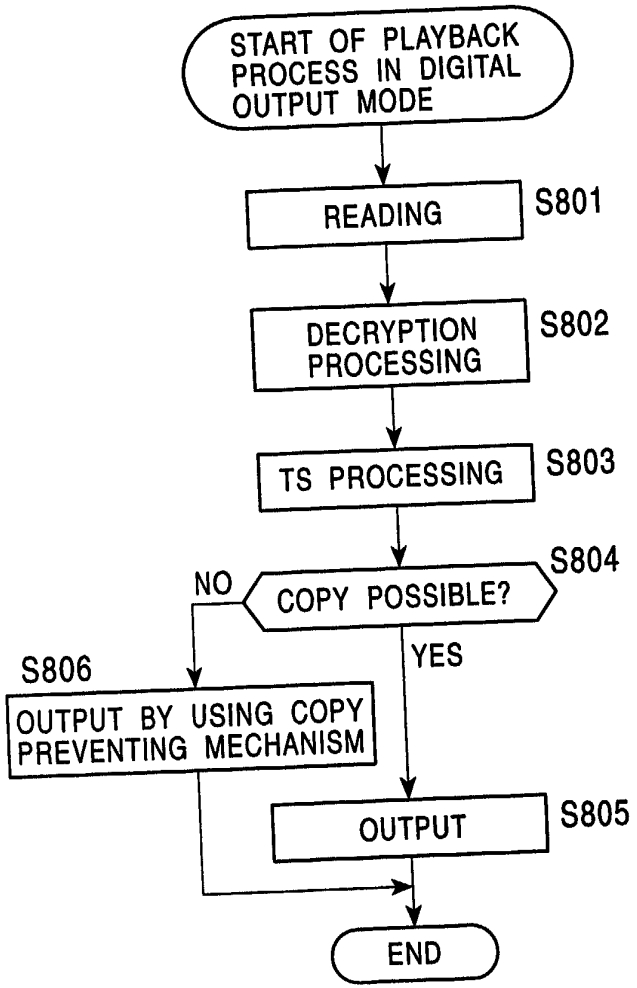


FIG. 34B

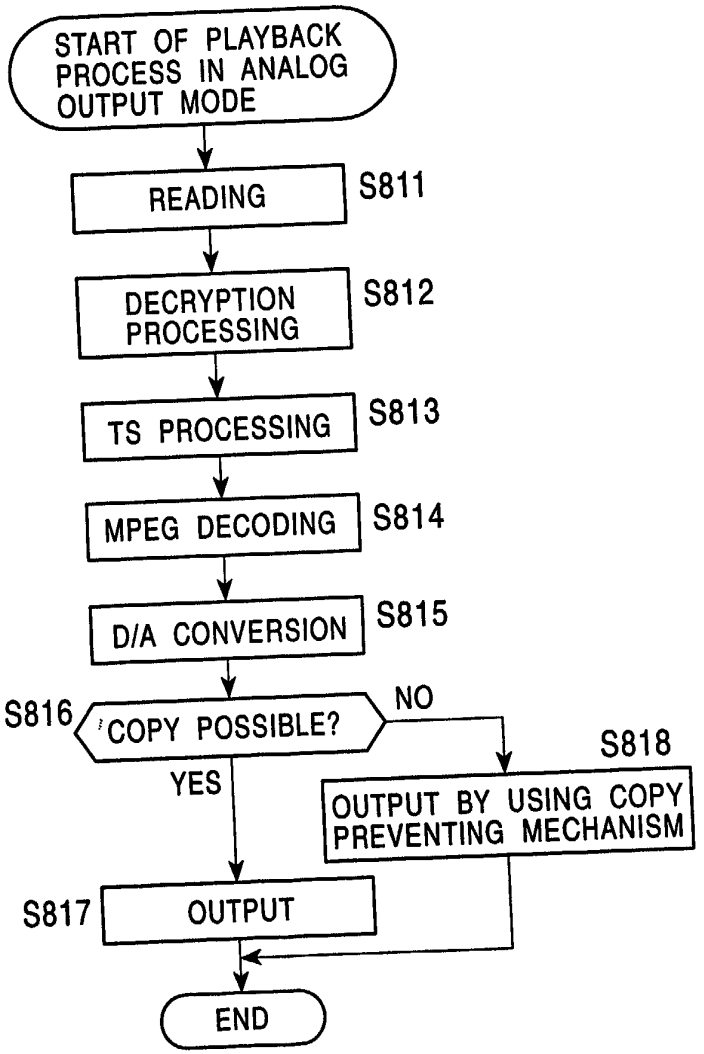
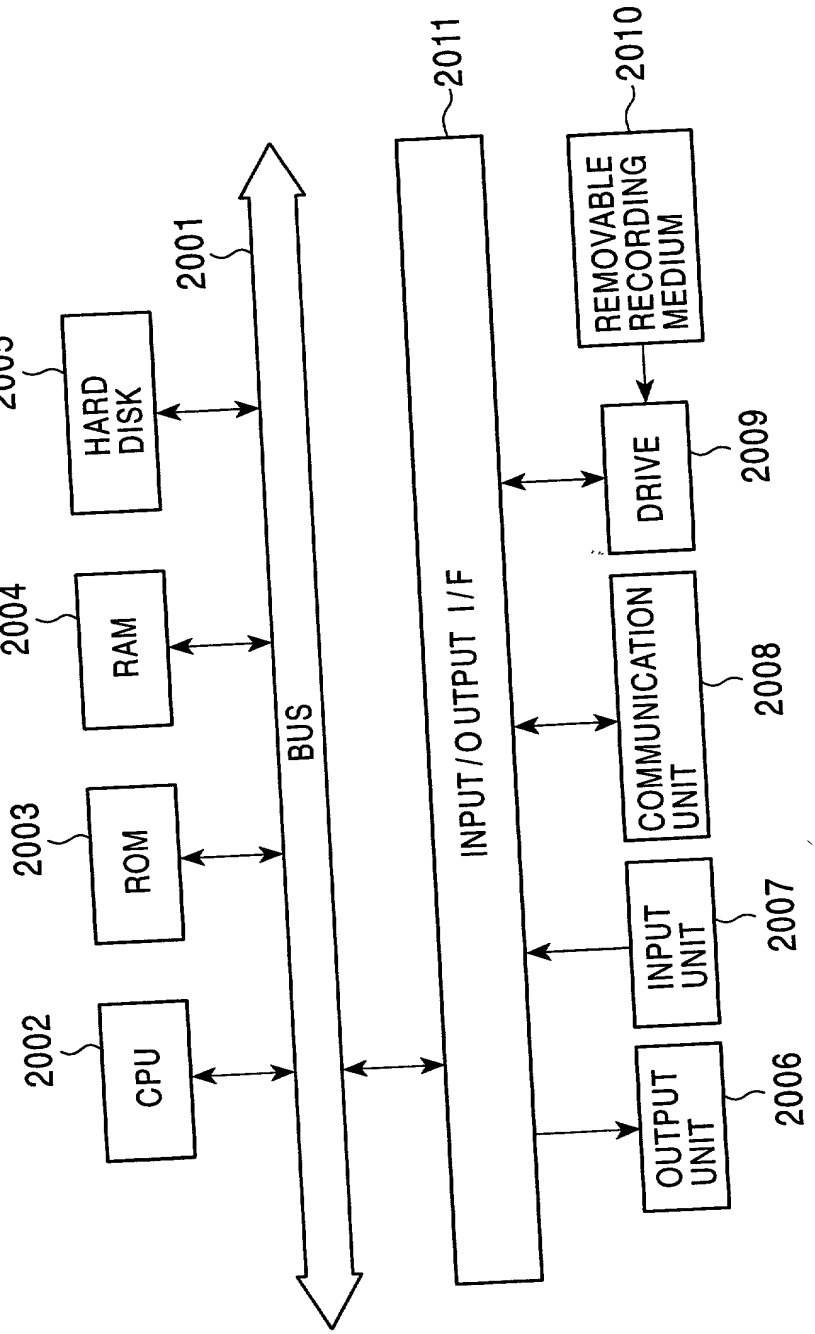


FIG. 35


2001
BUS
2002
CPU
2003
ROM
2004
RAM
2005
HARD DISK
2006
OUTPUT UNIT
2007
INPUT UNIT
2008
COMMUNICATION UNIT
2009
DRIVE
2010
REMOVABLE RECORDING MEDIUM
2011
INPUT/OUTPUT I/F